

**This Page Is Inserted by IFW Operations
and is not a part of the Official Record**

BEST AVAILABLE IMAGES

**Defective images within this document are accurate representation of
The original documents submitted by the applicant.**

Defects in the images may include (but are not limited to):

- **BLACK BORDERS**
- **TEXT CUT OFF AT TOP, BOTTOM OR SIDES**
- **FADED TEXT**
- **ILLEGIBLE TEXT**
- **SKEWED/SLANTED IMAGES**
- **COLORED PHOTOS**
- **BLACK OR VERY BLACK AND WHITE DARK PHOTOS**
- **GRAY SCALE DOCUMENTS**

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

This Page Blank (uspto)

DOCKET NO.: 209462 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: ISHIGURO, Ryuji et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HEREWITH

INTERNATIONAL APPLICATION NO.: PCT/JP00/07473

INTERNATIONAL FILING DATE: October 25, 2000

FOR: CONTENTS FURNISHING SYSTEM

REQUEST FOR CONSIDERATION OF DOCUMENTS
CITED IN INTERNATIONAL SEARCH REPORT

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir:

In the matter of the above-identified application for patent, notice is hereby given that applicant(s) request that the Examiner consider the documents cited in the International Search Report according to MPEP §609 and so indicate by a statement in the first Office Action that the information has been considered. When the Form PCT/DO/EO/903 indicates both the search report and copies of the documents are present in the national stage file, there is no requirement for the applicant(s) to submit them (1156 O.G. 91 November 23, 1993).

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Gregory J. Maier
Attorney of Record
Registration No. 21,124
Surinder Sachar
Registration No. 34,423



22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 1/97)

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/07473

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F15/00, H04L9/08, H04L9/32, G10K15/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F15/00, H04L9/08, H04L9/32, G10K15/02, G06F17/60, G11B 20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Toroku Jitsuyo Shinan Koho 1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, JICST Science Technology Document Database, INSPEC content, distribute, delivery, key, generation, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
EA	EP, 1001419, A1 (Matsushita Electric Ind. Co. Ltd.), 17 May, 2000 (17.05.00), Full text & WO, 2000/28539, A1 & JP, 2000-207835, A & BR, 9906815, A & NO, 200003492, A	1-10
EA	EP, 994404, A1 (Matsushita Electric Ind. Co. Ltd.), 19 April, 2000 (19.04.00), Full text & AU, 9952684, A & CN, 1263331, A & JP, 2000-348003, A	1-10
EA	JP, 2000-357201, A (Matsushita Electric Ind. Co., Ltd.), 26 December, 2000 (26.12.00), Full text (Family: none)	1-10
EA	JP, 2000-269950, A (Matsushita Electric Ind. Co., Ltd.), 29 September, 2000 (29.09.00), Full text (Family: none)	1-10

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family
---	--

Date of the actual completion of the international search
14 February, 2001 (14.02.01)

Date of mailing of the international search report
27 February, 2001 (27.02.01)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

THIS PAGE BLANK (USPTO)

PCT

国際調査報告

(法8条、法施行規則第40、41条)
[PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号 SK00PCT98	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220) 及び下記5を参照すること。	
国際出願番号 PCT/JP00/07473	国際出願日 (日.月.年) 25.10.00	優先日 (日.月.年) 25.10.99
出願人(氏名又は名称) ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 3 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☐ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 29 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

THIS PAGE BLANK (USPTO)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁷ G06F15/00, H04L9/08, H04L9/32, G10K15/02

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁷ G06F15/00, H04L9/08, H04L9/32, G10K15/02, G06F17/60, G11B 20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年

日本国公開実用新案公報 1971-2001年

日本国実用新案登録公報 1996-2001年

日本国登録実用新案公報 1994-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

WPI, JICST 科学技術文献データベース, INSPEC content, distribute, delivery, key, generation, authentication

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
EA	EP, 1001419, A1 (Matsushita Electric Ind. Co. Ltd.) 17. 5月.2000(17.05.00), 全頁を参照 & WO, 2000/28539, A1 & JP, 2000-207835, A & BR, 9906815, A & NO, 200003492, A	1-10
EA	EP, 994404, A1 (Matsushita Electric Ind. Co. Ltd.) 19. 4月.2000(19.04.00), 全頁を参照 & AU, 9952684, A & CN, 1263331, A & JP, 2000-348003, A	1-10
EA	JP, 2000-357201, A (松下電器産業株式会社) 26.12月.2000(26.12.00), 全頁を参照 (ファミリーなし)	1-10

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

14.02.01

国際調査報告の発送日

27.02.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正

5M

9364

電話番号 03-3581-1101 内線 3597

THIS PAGE BLANK (USPTO)

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
E A	JP, 2000-269950, A (松下電器産業株式会社) 29. 09月. 2000 (29. 09. 00), 全頁を参照 (ファミリーなし)	1-10

THIS PAGE BLANK (USPTO)

PCT COOPERATION TREATY

PCT

NOTIFICATION CONCERNING
SUBMISSION OR TRANSMITTAL
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

From the INTERNATIONAL BUREAU

To:

KOIKE, Akira
No. 11 Mori Building
6-4, Toranomom 2-chome
Minato-ku, Tokyo 105-0001
JAPON

Date of mailing (day/month/year) 17 November 2000 (17.11.00)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference SK00PCT98	
International application No. PCT/JP00/07473	International filing date (day/month/year) 25 October 2000 (25.10.00)
International publication date (day/month/year) Not yet published	Priority date (day/month/year) 25 October 1999 (25.10.99)
Applicant SONY CORPORATION et al	

1. The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).
2. This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.
3. An asterisk(*) appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b). In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.
4. The letters "NR" appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

<u>Priority date</u>	<u>Priority application No.</u>	<u>Country or regional Office or PCT receiving Office</u>	<u>Date of receipt of priority document</u>
25 Octo 1999 (25.10.99)	11/303142	JP	10 Nove 2000 (10.11.00)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer

Susumu Kubo

Telephone No. (41-22) 338.83.38

THIS PAGE BLANK (USPTO)

PCT COOPERATION TREATY

PCT

NOTICE INFORMING THE APPLICANT OF THE
COMMUNICATION OF THE INTERNATIONAL
APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

From the INTERNATIONAL BUREAU

To:

KOIKE, Akira
No. 11 Mori Building
6-4, Toranomom 2-chome
Minato-ku, Tokyo 105-0001
JAPON

Date of mailing (day/month/year) 03 May 2001 (03.05.01)		IMPORTANT NOTICE	
Applicant's or agent's file reference SK00PCT98			
International application No. PCT/JP00/07473	International filing date (day/month/year) 25 October 2000 (25.10.00)	Priority date (day/month/year) 25 October 1999 (25.10.99)	
Applicant SONY CORPORATION et al			

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
KR,US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
CA,CN,EP

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
03 May 2001 (03.05.01) under No. WO 01/31461

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a demand for international preliminary examination must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the national phase, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. (41-22) 740.14.35	Authorized officer J. Zahra Telephone No. (41-22) 338.83.38
--	---

THIS PAGE BLANK (USPTO)

OBLON, SPIVAK, McCLELLAND, MAIER, & NEUSTADT, P.C.**ATTORNEYS AT LAW****Fourth Floor****1755 Jefferson Davis Highway
Arlington, Virginia 22202 U.S.A.****Telephone: (703) 413-3000****Facsimile: (703) 413-2220****DATE: August 10, 2001****TO: Mrs. Wallace, U.S. PCT Branch****FACSIMILE NO.: (703) 305-3230****RE: U.S. Serial No: 09/857,218
Ryuji ISHIGURO et al.
Attorney Docket No. 209462US6PCT****NUMBER OF PAGES INCLUDING THIS PAGE: 2****FROM: Bette Snyder/Foreign Filing Department****OBLON, SPIVAK, McCLELLAND, MAIER & NEUSTADT, P.C.****Telephone: (703)-412-6237****COMMENTS: Per our conversation attached is the form PCT/IB/346 which acknowledges receipt of the Article 19 amendments by the International Bureau.****If you do not receive all pages, or, if they are not legible, please contact Bette Snyder at (703) 412-6237 immediately.****Thank you.**

THIS PAGE BLANK (USPTO)

PATENT COOPERATION TREATY

PCT

NOTIFICATION CONCERNING
THE FILING OF AMENDMENTS OF THE CLAIMS

(PCT Administrative Instructions, Section 417)

From the INTERNATIONAL BUREAU

To:

KOIKE, Akira
No. 11 Mori Building
6-4, Toranomon 2-chome
Minato-ku, Tokyo 105-0001
JAPON

Date of mailing (day/month/year) 26 April 2001 (26.04.01)	
Applicant's or agent's file reference SK00PCT98	IMPORTANT NOTIFICATION
International application No. PCT/JP00/07473	International filing date (day/month/year) 25 October 2000 (25.10.00)
Applicant SONY CORPORATION et al	

1. The applicant is hereby notified that amendments to the claims under Article 19 were received by the International Bureau on:

24 April 2001 (24.04.01)

2. This date is within the time limit under Rule 46.1.

Consequently, the international publication of the international application will contain the amended claims according to Rule 48.2(f), (h) and (i).

3. The applicant is reminded that the international application (description, claims and drawings) may be amended during the international preliminary examination under Chapter II, according to Article 34, and in any case, before each of the designated Offices, according to Article 28 and Rule 52, or before each of the elected Offices, according to Article 41 and Rule 78.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorised officer

Susumu Kubo

Telephone No.: (41-22) 338.83.38

THIS PAGE BLANK (USPTO)

*** RX REPORT ***

RECEPTION OK

TX/RX NO	9987
CONNECTION TEL	
SUBADDRESS	
CONNECTION ID	
ST. TIME	08/10 15:01
USAGE T	00'40
PGS.	2
RESULT	OK

THIS PAGE BLANK (USPTO)

09/857218

531 Rec'd PCT 22 JUN 2001

THE FOLLOWING IS THE ENGLISH TRANSLATION OF THE
AMENDMENTS TO THE CLAIMS OF THE INTERNATIONAL
APPLICATION UNDER PCT ARTICLE 19:

AMENDED SHEETS

(Pages 77, 78, 79, 80, 81, 81a, 81b, 81c, 81d, 81e, 81f, 81g, 81h, 81i, 81j, 81k,
81l and 81m)

THIS PAGE BLANK (USPTO)

CLAIMS

1. A contents purveying system including a data processor having a reproduction program for reproducing contents data, a portable reproducing device for storing the contents data furnished from said data processor on a recording medium for reproduction and a contents server for distributing the contents data over a network to said data processor, wherein said data processor is configured so that

6/11/11 by [signature]
a first master key and a first authentication key are furnished to said reproduction program after installing said reproduction program, the contents data stored in an external storage medium connected to the data processor are acquired using said first master key for storage, said reproduction program executing authentication with respect to said portable reproducing device using the so-furnished first authentication key and first master key,

said data processor also being configured so that, when transmission/reception of the contents data distributed from said contents server to said reproduction program is made with said portable reproducing device, a second master key different from said first master key and a second authentication key different from the first authentication key are furnished over the network, the contents data furnished from said contents server are acquired using the so-furnished second master key for storage, and authentication with respect to the portable reproducing device is made using the so-furnished second authentication key and the second master key to effect transmission/reception of the contents data.

THIS PAGE BLANK (USPTO)

2. The contents purveying system according to claim 1 wherein said portable reproducing device holds first to i'th authentication keys updated in generation from the first to the i'th generation, i being an integer equal to 2 or larger, and first to i'th master keys updated in generation from the first to the i'th generation, i being an integer equal to 2 or larger;

said reproducing program being furnished over the network with second to i'th authentication keys updated in generation from the second to the i'th generation, i being an integer equal to 2 or larger, and second to i'th master keys updated in generation from the second to the i'th generation, i being an integer equal to 2 or larger;

said portable reproducing device performing reciprocal authentication with said reproduction program using the authentication key of the same generation.

3. The contents purveying system according to claim 2 wherein if said portable reproducing device performing reciprocal authentication with said reproduction program is using an authentication key and a master key of a generation older than the generation used by said reproduction program, the portable reproducing device updates the own authentication key and master key until the generation used by said reproduction program.

4. The contents purveying system according to claim 2 wherein if said reproduction program performing reciprocal authentication with said portable reproducing device is using an authentication key and a master key of a generation older than that used by

THIS PAGE BLANK (USPTO)

said portable reproducing device, said reproduction program asks said contents server for a key to update the own authentication key and the own master key up to the generation used by said portable reproducing device.

5. The contents purveying system according to claim 2 wherein, if accessed by said contents server, said contents server furnishes an authentication key and a master key of a generation later than that of the authentication key used by said reproduction program to update the generation of the authentication key used by said reproduction program.

6. A contents purveying method including a data processor having a reproduction program for reproducing contents data, a portable reproducing device for storing the contents data furnished from said data processor on a recording medium for reproduction and a contents server for distributing the contents data over a network to said data processor, wherein

a first master key and a first authentication key are furnished to said reproduction program after installing said reproduction program, the contents data stored in an external storage medium connected to the data processor are acquired using said first master key for storage, said reproduction program executing authentication with respect to said portable reproducing device using the so-furnished first authentication key and first master key, and wherein

when transmission/reception of the contents data distributed from said contents server to said reproduction program is made with said portable reproducing device, a

THIS PAGE BLANK (USPTO)

second master key different from said first master key and a second authentication key different from the first authentication key are furnished over the network, the contents data furnished from said contents server are acquired using the so-furnished second master key for storage, and authentication with respect to the portable reproducing device is made using the so-furnished second authentication key and the second master key to effect transmission/reception of the contents data.

7. The contents purveying method according to claim 6 wherein said portable reproducing device holds first to i 'th authentication keys updated in generation from the first to the i 'th generation, i being an integer equal to 2 or larger, and first to i 'th master keys updated in generation from the first to the i 'th generation, i being an integer equal to 2 or larger;

said reproducing program being furnished over the network with second to i 'th authentication keys updated in generation from the second to the i 'th generation, i being an integer equal to 2 or larger, and second to i 'th master keys updated in generation from the second to the i 'th generation, i being an integer equal to 2 or larger;

said portable reproducing device performing reciprocal authentication with said reproduction program using the authentication key of the same generation.

8. The contents purveying method according to claim 7 wherein if said portable reproducing device performing reciprocal authentication with said reproduction program is using an authentication key and a master key of a generation older than the

THIS PAGE BLANK (USPTO)

generation used by said reproduction program, the portable reproducing device updates the own authentication key and the own master key up to the generation used by said reproduction program.

9. The contents purveying method according to claim 7 wherein if said reproduction program performing reciprocal authentication with said portable reproducing device is using an authentication key and a master key of a generation older than that used by said portable reproducing device, said reproduction program asks said contents server for a key to update the own authentication key and the own master key up to the generation used by said portable reproducing device.

10. The contents purveying method according to claim 7 wherein, if accessed by said contents server, said contents server furnishes an authentication key and a master key of a generation later than that of the authentication key used by said reproduction program to update the generation of the authentication key used by said reproduction program.

THIS PAGE BLANK (USPTO)

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001年5月3日 (03.05.2001)

PCT

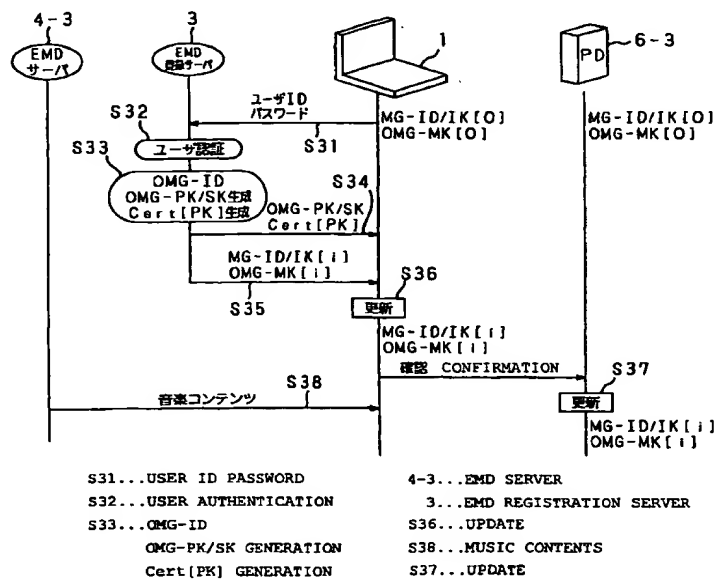
(10) 国際公開番号
WO 01/31461 A1

- (51) 国際特許分類⁷: G06F 15/00, H04L 9/08, 9/32, G10K 15/02
- (21) 国際出願番号: PCT/JP00/07473
- (22) 国際出願日: 2000年10月25日 (25.10.2000)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願平 11/303142
1999年10月25日 (25.10.1999) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 石黒隆二 (ISHIGURO, Ryuji) [JP/JP]. 河上 達 (KAWAKAMI, Itaru) [JP/JP]. 田辺 充 (TANABE, Mitsuru) [JP/JP]. 江面裕一 (EZURA, Yuichi) [JP/JP]. 佐藤一郎 (SATO, Ichiro) [JP/JP]. 海老原宗毅 (EBIHARA, Munetake) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (74) 代理人: 小池 晃, 外 (KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).
- (81) 指定国 (国内): CA, CN, KR, US.
- (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
- 添付公開書類:
— 国際調査報告書

[続葉有]

(54) Title: CONTENTS PROVIDING SYSTEM

(54) 発明の名称: コンテンツ提供システム



(57) Abstract: A reproduction program is installed in a PC, and then a ripping key of a CD is provided from, e.g. an FD. By using the ripping key, the music contents in the CD can be copied to a PD, but music contents cannot be downloaded from an EMD server and copied to a PD. If the music contents distributed from an EMD server is stored in a PD, a key for EMD different from the ripping key is acquired through a network and the reproduction program is executed. Thus, the security of the contents data distributed through a network is enhanced.

[続葉有]

WO 01/31461 A1



— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

再生プログラムは、P C上にインストールされた後に、C Dのリップping用の鍵が例えばF Dから提供される。このC Dのリップping用の鍵では、C D内の音楽コンテンツをP Dにコピーはできるが、E M Dサーバから音楽コンテンツをダウンロードしてP Dにコピーすることはできない。再生プログラムは、E M Dサーバから配信された音楽コンテンツをP Dに保存する場合には、リップping用の鍵とは異なるE M D用の鍵をネットワークを介して取得したのちに行う。このようにすることにより、ネットワークを介して配信されたコンテンツデータの安全性を高められる。

明細書

コンテンツ提供システム

技術分野

半導体メモリやメモリカード等を記憶媒体とした可搬再生装置にコンテンツデータを提供するコンテンツ提供システム及びコンテンツ提供方法に関するものである。

背景技術

近年、インターネットやケーブルテレビ等のネットワークを用いた音楽コンテンツのオンライン配信が実用化され始めた。

このような音楽コンテンツの配信システムにおいては、コンテンツ配信業者は、音楽コンテンツをネットワークを介して配信する場合、例えば、Web上に音楽コンテンツを提供する。また、この音楽配信システムを利用するユーザは、自己のパーソナルコンピュータを用いて、コンテンツ配信業者が提供するWeb等にアクセスをして、所望の音楽コンテンツをダウンロードする。ユーザは、取得した音楽コンテンツを、例えば、パーソナルコンピュータ内のプレーヤアプリケーションにより再生したり、また、このパーソナルコンピュータと接続可能なポータブルデバイス等により再生する。

ここで、コンテンツ提供業者は、そのコンテンツの著作権を管理しなければならない。そのため、コンテンツ配信業者は、インターネットを介してWeb上にアクセスしてきたユーザをID情報や暗証番号等で認識し、正当なユーザに対してのみに暗号化した音楽コ

ンテンツを配信する。そして、その音楽コンテンツは、ユーザからは自由に参照できないような暗号鍵により鍵管理がされた状態で、パーソナルコンピュータ内のハードディスクに格納される。また、パーソナルコンピュータ内に格納された音楽コンテンツをポータブルデバイスに転送する場合には、プレーヤアプリケーションとポータブルデバイスとの間で認証処理を行った後に、ポータブルデバイスが有する記憶媒体に音楽コンテンツが格納される。

ところで、一般に、ポータブルデバイスには、ネットワークから配信された音楽コンテンツのみならず、例えばCD等のメディアから音楽コンテンツをコピーすることもできる。

ところが、従来、ポータブルデバイスとパーソナルコンピュータと間の認証の方式は、CD等のメディアからコピーされた音楽コンテンツのみを扱うプレーヤアプリケーションであろうが、ネットワークからダウンロードした音楽コンテンツを扱うプレーヤアプリケーションであろうが、特に区別がされず行われていた。

そのため、例えば、なんらかの悪意を有する者により、ポータブルデバイスとパーソナルコンピュータとの認証鍵が破られた場合、CD等のメディアからコピーされた音楽コンテンツと、ネットワークを介して配信した音楽コンテンツとの両者ともに不正にコピーがされてしまう。

特に、CD等のメディアの場合は、一般にメディアが販売された時に課金が終了している場合が主であるが、ネットワークを介して配信された音楽コンテンツは、例えば、再生をした回数や複製をした回数等に応じて課金等がされる場合があり、より強固な鍵管理が望まれる。

発明の開示

本発明は、ネットワークを介して配信されたコンテンツデータの安全性を高めることができるコンテンツ提供システム及びコンテンツ提供方法を提供することを目的とする。

本発明にかかるコンテンツ提供システムは、コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとからなるコンテンツ提供システムにおいて、上記データ処理装置は、上記再生プログラムがインストールされた後に、第1のマスター鍵及び第1の認証鍵が上記再生プログラムに提供され、上記第1のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第1の認証鍵及び第1のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、上記再生プログラムが上記コンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第1のマスター鍵とは異なる第2のマスター鍵及び上記第1の認証鍵とは異なる第2の認証鍵がネットワークを介して提供され、この提供された第2のマスター鍵を用いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第2の認証鍵及び第2のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うことを特徴とする。

コンテンツ提供システムでは、再生プログラムが、外部記憶媒体に格納されたコンテンツデータのみを取り扱う場合には、第１の認証鍵及び第１のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。再生プログラムが、ネットワークを介して提供されたコンテンツデータを取り扱う場合には、第１の認証鍵及び第１のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。第２の認証鍵及び第２のマスター鍵は、ネットワークを介して再生プログラムに提供され、第１の認証鍵及び第１のマスター鍵と異なる鍵となっている。

本発明にかかるコンテンツ提供方法は、コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置とによりユーザにコンテンツデータを提供するコンテンツサーバとからなるコンテンツ提供方法において、上記再生プログラムをインストールした後に、第１のマスター鍵及び第１の認証鍵が上記再生プログラムに提供され、上記第１のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第１の認証鍵及び第１のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、上記再生プログラムがコンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第１のマスター鍵とは異なる第２のマスター鍵及び上記第１の認証鍵とは異なる第２の認証鍵がネットワークを介して提供され、この提供された第２のマスター鍵を用

いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第2の認証鍵及び第2のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うことを特徴とする。

このコンテンツ提供方法では、再生プログラムが、外部記憶媒体に格納されたコンテンツデータのみを取り扱う場合には、第1の認証鍵及び第1のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。再生プログラムが、ネットワークを介して提供されたコンテンツデータを取り扱う場合には、第1の認証鍵及び第1のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。第2の認証鍵及び第2のマスター鍵は、ネットワークを介して再生プログラムに提供され、第1の認証鍵及び第1のマスター鍵と異なる鍵となっている。

図面の簡単な説明

図1は、本発明の実施の形態の音楽コンテンツ配信システムの構成を示す図である。

図2は、上記音楽コンテンツ配信システムにおけるパーソナルコンピュータの構成を示す図である。

図3は、上記音楽コンテンツ配信システムにおけるポータブルデバイスの構成を示す図である。

図4は、上記パーソナルコンピュータの機能について説明する図である。

図5は、表示操作指示ウィンドウの一例を示す図である。

図 6 は、録音プログラムがディスプレイに表示させる表示例を示す図である。

図 7 は、上記音楽コンテンツ配信システムにおける、配信業者毎にフォーマットが異なるコンテンツの統一的な取り扱いについて説明するための図である。

図 8 は、統一転送プロトコルレイヤとアプリケーションレイヤとの関係を説明する図である。

図 9 A 及び図 9 B は、一般的に用いられる利用条件情報のフォーマットを説明する図である。

図 10 は、包括管理ユニットで用いられる統一利用条件情報を構成するファイルを説明する図である。

図 11 は、上記統一利用条件情報のオートマトンファイルの構成を説明する図である。

図 12 は、上記オートマトンファイルのオートマトン記述部に記述される音楽コンテンツの動作遷移を示すオートマトンの一例を説明する図である。

図 13 は、図 12 で示した上記オートマトンを `t u p l e` 列で表現した図である。

図 14 は、上記オートマトン記述部の構成を説明する図である。

図 15 は、XML の仕様に基づいて規定された DTD で定義されているイベントとコマンドとを示す図である。

図 16 は、上記オートマトン記述部の第 1 の記述例を示す図である。

図 17 は、上記第 1 の記述例の状態遷移図である。

図 18 は、上記オートマトン記述部の第 2 の記述例を示す図であ

る。

図 1 9 は、上記第 2 の記述例の状態遷移図である。

図 2 0 は、上記オートマトン記述部の第 3 の記述例を示す図である。

図 2 1 は、上記第 3 の記述例の状態遷移図である。

図 2 2 は、上記オートマトン記述部の第 4 の記述例を示す図である。

図 2 3 は、上記統一利用条件情報のパラメータファイルの構成を説明する図である。

図 2 4 は、上記パラメータファイルを更新した場合の構成を説明する図である。

図 2 5 は、上記パラメータファイルのパラメータ記述部の構成を説明する図である。

図 2 6 は、上記包括管理ユニットによるコンテンツの管理方法について説明する図である。

図 2 7 は、包括管理ユニットが C D - R O M からインストールされる場合の処理手順について説明する図である。

図 2 8 は、包括管理ユニットがネットワークからダウンロードされてインストールされる場合の処理手順について説明する図である。

図 2 9 は、リッピング鍵から E M D 鍵に更新する更新手順について説明する図である。

図 3 0 は、E M D 鍵を更新する手順の第 1 の例について説明する図である。

図 3 1 は、E M D 鍵を更新する手順の第 2 の例について説明する図である。

発明を実施するための最良の形態

以下、本発明の最良の実施の形態として、本発明を適用した音楽コンテンツ配信システムについて図面を参照しながら詳細に説明する。この音楽コンテンツ配信システムは、ネットワークを介してサーバからパーソナルコンピュータやポータブルデバイスにダウンロードし、さらに、ダウンロードした音楽コンテンツやCDから読みとった音楽コンテンツの管理等を行うシステムである。

(1) 音楽コンテンツ配信システムの全体構成

図1は、本発明を適用した音楽コンテンツ配信システムの全体構成を示す図である。

この音楽コンテンツ配信システムは、パーソナルコンピュータ1と、インターネットやローカルエリアネットワーク等のネットワーク2と、登録サーバ3と、音楽データ（以下、コンテンツと呼ぶ。）を配信する複数のEMD（Electrical Music Distribution）サーバ4（4-1，4-2，4-3）と、WWWサーバ5（5-1，5-2）とを備えて構成される。また、パーソナルコンピュータ1には、USBケーブル7（7-1，7-2，7-3）を介して、内部にメモリーカード等の記憶媒体が格納され、コンテンツの再生を行う携帯型の音楽再生器機であるポータブルデバイス6（6-1，6-2，6-3）が接続される。

パーソナルコンピュータ1は、ネットワーク2を介して、EMD登録サーバ3、EMDサーバ4（4-1，4-2，4-3）、WWW（World Wide Web）サーバ5（5-1，5-2）と接続される。

パーソナルコンピュータ1は、EMDサーバ4（4-1，4-2，

4-3) から、所定の圧縮方式で圧縮されたコンテンツを受信し、所定の暗号化方式で暗号化して記録する。また、パーソナルコンピュータ 1 は、CD (Compact Disc) 等から読みとったコンテンツを、所定の圧縮方式で圧縮して、所定の暗号化方式で暗号化して記録する。圧縮方式としては、例えば A T R A C (Adaptive Transform Acoustic Coding) 3 (商標) や M P 3 (MPEG Audio Layer -3) 等の方式が用いられる。また、暗号化方式としては、D E S (Data Encryption Standard) などが用いられる。

また、パーソナルコンピュータ 1 は、コンテンツの配信を受ける場合には、そのコンテンツの利用条件を示す利用条件情報の配信も受け、それを記録する。また、パーソナルコンピュータ 1 は、CD 等から読みとったコンテンツを記録する場合には、そのコンテンツの再生条件に応じて、利用条件情報を生成して、それを記録する。

また、パーソナルコンピュータ 1 は、暗号化して記録しているコンテンツを、利用条件情報及び曲名や演奏者等の関連情報とともに、U S B ケーブル 7 (7-1, 7-2, 7-3) を介して、ポータブルデバイス 6 (6-1, 6-2, 6-3) に記録し、記憶させたことに対応して利用条件情報を更新する。この処理のことをチェックアウトという。利用条件情報は、チェックアウトしたとき、パーソナルコンピュータ 1 が記録している、そのコンテンツのチェックアウト可能回数を 1 減少させる。チェックアウト可能回数が 0 のときには、対応するコンテンツは、チェックアウトすることができない。

また、パーソナルコンピュータ 1 は、U S B ケーブル 7 (7-1, 7-2, 7-3) を介して、ポータブルデバイス 6 (6-1, 6-2, 6-3) に記憶されているコンテンツを、消去し (または、使

用できなくさせ)、消去したことに対応させて利用条件情報を更新する。この消去処理のことをチェックインと呼ぶ。チェックインしたとき、パーソナルコンピュータ1が記録している、そのコンテンツのチェックアウト可能回数を1増加させる。

なお、パーソナルコンピュータ1は、他のパーソナルコンピュータがポータブルデバイス6にチェックアウトしたコンテンツに対してはチェックインはできない。すなわち、パーソナルコンピュータ1自身がチェックアウトしたコンテンツしか、チェックインをすることができない。

EMD登録サーバ3は、パーソナルコンピュータ1がEMDサーバ4(4-1, 4-2, 4-3)からコンテンツの取得を開始するとき、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、パーソナルコンピュータ1とEMDサーバ4(4-1, 4-2, 4-3)との相互認証に必要な認証鍵をパーソナルコンピュータ1に送信するとともに、EMDサーバ4(4-1, 4-2, 4-3)に接続するためのプログラムをパーソナルコンピュータ1に送信する。

EMDサーバ4(4-1, 4-2, 4-3)は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、利用条件情報及びコンテンツの関連データ(例えば、曲名、又は演奏者など)とともに、パーソナルコンピュータ1にコンテンツを供給する。

各EMDサーバ4(4-1, 4-2, 4-3)が配信するコンテンツは、所定の圧縮の方式で圧縮されている。その圧縮方式は、サーバ毎に異なってもよい。また、各EMDサーバ4(4-1, 4-2, 4-3)が供給するコンテンツは、所定の暗号化方式で暗

号化されて配信される。その暗号化方式は、サーバ毎に異なっているともよい。

WWWサーバ5（5-1，5-2）は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツを読み取ったCD（例えば、CDのアルバム名、又はCDの販売会社など）及びCDから読み取ったコンテンツに対応するデータ（例えば、曲名、又は作曲者名など）をパーソナルコンピュータ1に供給する。

ポータブルデバイス6（6-1，6-2，6-3）は、パーソナルコンピュータ1から供給されたコンテンツ（すなわち、チェックアウトされたコンテンツ）を再生し、図示せぬヘッドフォンなどに出力する装置である。

各ポータブルデバイス6（6-1，6-2，6-3）は、コンテンツを記憶するための記憶媒体を有している。記憶媒体としては、例えば、装置の内部基板に装着された取り外しが不可能なICメモリや、着脱が可能なメモリカード等が用いられる。ポータブルデバイス6（6-1，6-2，6-3）は、USB等の物理的なインターフェース7（7-1，7-2，7-3）を介してパーソナルコンピュータ1と接続され、コンテンツが転送される。このとき、コンテンツは、暗号化及び圧縮された状態で転送され、利用条件情報も付加されている。

各ポータブルデバイス6（6-1，6-2，6-3）は、通常、パーソナルコンピュータ1との接続が切り離された状態で用いられ、この状態でユーザにより再生命令が与えられると、暗号化したコンテンツを記憶媒体から読み出し、再生をする。また、各ポータブルデバイス6（6-1，6-2，6-3）は、各コンテンツに付加さ

れている利用条件情報に基づき、また、必要に応じて再生の制限を行ったり、コンテンツの削除等の制御を行ったり、利用条件情報の更新等を行う。

以下、ポータブルデバイス 6-1, 6-2, 6-3 を個々に区別する必要がないとき、単にポータブルデバイス 6 と称する。

つぎに、図 2 を参照して、パーソナルコンピュータ 1 の構成について説明をする。

CPU (Central Processing Unit) 11 は、各種アプリケーションプログラム (詳細については後述する。) や、OS (Operating System) を実際に実行する。ROM (Read - only Memory) 12 は、一般的には、CPU 11 が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random Access Memory) 13 は、CPU 11 の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらは CPU バスなどから構成されるホストバス 14 により相互に接続されている。

ホストバス 14 は、ブリッジ 15 を介して、PCI (Peripheral Component Interconnect / Interface) バスなどの外部バス 16 に接続されている。

キーボード 18 は、CPU 11 に各種の指令を入力するとき、使用者により操作される。マウス 19 は、ディスプレイ 20 の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ 20 は、液晶表示装置又は CRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。HDD (Hard Disk Drive) 21 は、ハードディスクを駆動し、それら

にCPU 11によって実行するプログラムや情報を記録又は再生させる。

ドライブ22は、装着されている磁気ディスク41、光ディスク42（CDを含む）、光磁気ディスク43、又は半導体メモリ44に記録されているデータ又はプログラムを読み出して、そのデータ又はプログラムを、インターフェース17、外部バス16、ブリッジ15及びホストバス14を介して接続されているRAM13に供給する。

USBポート23（23-1，23-2，23-3）には、USBケーブル7（7-1，7-2，7-3）を介して、ポータブルデバイス6（6-1，6-2，6-3）が接続される。USBポート23は、インターフェース17、外部バス16、ブリッジ15、又はホストバス14を介して、HDD21、CPU11、又はRAM13から供給されたデータ（例えば、コンテンツ又はポータブルデバイス6のコマンドなどを含む）をポータブルデバイス6（6-1，6-2，6-3）に出力する。

IEC（International Electrotechnical Commission）60958端子24aを有する音声入出力インタフェース24は、デジタル音声入出力、あるいはアナログ音声入出力のインタフェース処理を実行する。スピーカ45は、音声入出力インタフェース24から供給された音声信号を基に、コンテンツに対応する所定の音声を出力する。

これらのキーボード18、マウス19、ディスプレイ20、HDD21、ドライブ22、USBポート23、音声入出力インタフェース24は、インターフェース17に接続されており、インターフ

エース 17 は、外部バス 16、ブリッジ 15 及びホストバス 14 を介して CPU 11 に接続されている。

通信部 25 は、ネットワーク 2 が接続され、CPU 11、又は HDD 21 から供給されたデータ（例えば、登録の要求、又はコンテンツの送信要求など）を、所定の方式の packets に格納して、ネットワーク 2 を介して、送信するとともに、ネットワーク 2 を介して、受信した packets に格納されているデータ（例えば、認証鍵、又はコンテンツなど）を CPU 11、RAM 13、又は HDD 21 に出力する。

半導体 IC として、一体的に形成され、パーソナルコンピュータ 1 に装着されるアダプタ 26 の CPU 32 は、外部バス 16、ブリッジ 15 及びホストバス 14 を介してパーソナルコンピュータ 1 の CPU 11 と共働し、各種の処理を実行する。RAM 33 は、CPU 32 が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ 34 は、パーソナルコンピュータ 1 の電源がオフされた後も保持する必要があるデータを記憶する。ROM 36 には、パーソナルコンピュータ 1 から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC (Real Time Clock) 35 は、計時動作を実行し、時刻情報を提供する。半導体 IC は、セキュアな環境に設計されており、外部からの悪意なアクセスに対して耐性をもっている。なお、この機能は、ソフトウェアプログラムで構成されていてもよい。

通信部 25 及びアダプタ 26 は、外部バス 16、ブリッジ 15 及びホストバス 14 を介して CPU 11 に接続されている。

次に、図 3 を参照して、ポータブルデバイス 6 の構成を説明する。

電源回路 5 2 は、乾電池 5 1 から供給される電源電圧を所定の電圧の内部電力に変換して、CPU 5 3 ～表示部 6 7 に供給することにより、ポータブルデバイス 6 全体を駆動させる。

USB コントローラ 5 7 は、USB コネクタ 5 6 を介して、パーソナルコンピュータ 1 と USB ケーブル 7 を介して接続された場合、パーソナルコンピュータ 1 から転送されたコンテンツを含むデータを、内部バス 5 8 を介して、CPU 5 3 に供給する。

パーソナルコンピュータ 1 から転送されるデータは、1 パケット当たり 6 4 バイトのデータから構成され、1 2 M b i t / s e c の転送レートでパーソナルコンピュータ 1 から転送される。

ポータブルデバイス 6 に転送されるデータは、ヘッダ及びコンテンツから構成される。ヘッダには、コンテンツ ID、ファイル名、ヘッダサイズ、コンテンツ鍵、ファイルサイズ、コーデック ID、ファイル情報などが格納されているとともに、再生制限処理等に必要な利用条件情報等が格納されている。コンテンツは、A T R A C 3 などの符号化方式で符号化され、暗号化されている。

ヘッダサイズは、ヘッダのデータ長（例えば、3 3 バイトなど）を表し、ファイルサイズは、コンテンツのデータ長（例えば、3 3 , 6 3 6 , 1 3 8 バイトなど）を表す。

コンテンツ鍵は、暗号化されているコンテンツを復号するための鍵であり、パーソナルコンピュータ 1 とポータブルデバイス 6 との相互認証の処理で生成されたセッション鍵（一時鍵）を基に暗号化された状態で、パーソナルコンピュータ 1 からポータブルデバイス 6 に送信される。

ポータブルデバイス 6 が U S B ケーブル 7 を介してパーソナルコンピュータ 1 の U S B ポート 2 3 に接続されたとき、ポータブルデバイス 6 とパーソナルコンピュータ 1 とは、相互認証の処理を実行する。この相互認証の処理は、例えば、チャレンジレスポンス方式の認証の処理である。ちなみに、ポータブルデバイス 6 の D S P 5 9 は、チャレンジレスポンス方式の認証の処理を行うとき、暗号解読（復号）の処理を実行する。

チャレンジレスポンス方式とは、例えば、パーソナルコンピュータ 1 が生成するある値（チャレンジ）に対して、ポータブルデバイス 6 がパーソナルコンピュータ 1 と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。チャレンジレスポンス方式の相互認証の処理においては、パーソナルコンピュータ 1 が生成する値は認証の処理毎に毎回変化するもので、例えば、ポータブルデバイス 6 が出力した、秘密鍵を使用して生成された値が読み出されて、いわゆる、なりすましの攻撃を受けても、次の相互認証の処理では、相互認証に使用される値が異なるので、パーソナルコンピュータ 1 は不正を検出できる。

コンテンツ I D は、コンテンツに対応した、コンテンツを特定するための I D である。

コーデック I D は、コンテンツの符号化方式に対応した I D であり、例えば、コーデック I D ” 1 ” は、A T R A C 3 に対応し、コーデック I D ” 0 ” は、M P 3 （MPEG（Moving Picture Experts Group） Audio Layer-3）に対応する。

ファイル名は、コンテンツに対応するパーソナルコンピュータ 1 が記録しているコンテンツファイル（後述する）を A S C I I （ A

merican National Standard Code for Information Interchange)

コードに変換したデータであり、ファイル情報は、コンテンツに対応する曲名、アーティスト名、作詞者名、又は作曲者名などをASCIIコードに変換したデータである。

ポータブルデバイス6が、パーソナルコンピュータ1からコンテンツとともにコンテンツの書き込み命令を受信した場合、RAM54又はROM55から読み出したメインプログラムを実行するCPU53は、書き込み命令を受け取り、フラッシュメモリコントローラ60を制御して、パーソナルコンピュータ1から受信したコンテンツをフラッシュメモリ61に書き込ませる。

フラッシュメモリ61は、約64MByteの記憶容量を有し、コンテンツを記憶する。また、フラッシュメモリ61には、所定の圧縮方式で圧縮されているコンテンツを伸張するための再生用コードが予め格納されている。

なお、フラッシュメモリ61は、ポータブルデバイス6にメモ리카ードとして着脱可能とすることができるようにしてもよい。

使用者による、図示せぬ再生/停止ボタンの押し下げ操作に対応した再生命令が操作キーコントローラ62を介してCPU53に供給されると、CPU53は、フラッシュメモリコントローラ60に、フラッシュメモリ61から、再生用コードとコンテンツとを読み出させ、DSP59に転送させる。

DSP59は、フラッシュメモリ61から転送された再生用コードに基づいてコンテンツをCRC (Cyclic Redundancy Check) 方式で誤り検出をした後、再生して、再生したデータ (図3中においてD1で示す) をディジタル/アナログ変換回路63に供給する。

DSP 59は、内部に設けられた発信回路とともに一体に構成され、外付けされた水晶で成る発信子59AからのマスタークロックMCLKを基に、コンテンツを再生するとともに、マスタークロックMCLK、マスタークロックMCLKを基に内部の発振回路で生成した所定の周波数のビットクロックBCLK、並びに、フレーム単位のLチャンネルクロックLCLK及びRチャンネルクロックRCLKからなる動作クロックLRCLKをディジタルアナログ変換回路63に供給する。

DSP 59は、コンテンツを再生するとき、再生用コードに従って上述の動作クロックをディジタルアナログ変換回路63に供給して、コンテンツを再生しないとき、再生用コードに従って動作クロックの供給を停止して、ディジタルアナログ変換回路63を停止させて、ポータブルデバイス6全体の消費電力量を低減する。

同様に、CPU 53及びUSBコントローラ57も、水晶でなる発振子53A又は57Aがそれぞれ外付けされ、発振子53A又は57Aからそれぞれ供給されるマスタークロックMCLKに基づき、所定の処理を実行する。

このように構成することで、ポータブルデバイス6は、CPU 53、DSP 59、USBコントローラ57等の各回路ブロックに対してクロック供給を行うためのクロック発生モジュールが不要となり、回路構成を簡素化するとともに小型化することができる。

ディジタルアナログ変換回路63は、再生したコンテンツをアナログの音声信号に変換して、これを増幅回路64に供給する。増幅回路64は、音声信号を増幅して、ヘッドフォンジャック65を介して、ヘッドフォンに音声信号を供給する。

このように、ポータブルデバイス 6 は、再生／停止ボタンが押圧操作されたとき、CPU 53 の制御に基づいてフラッシュメモリ 61 に記憶されているコンテンツを再生するとともに、再生中に再生／停止ボタンが押圧操作されたとき、コンテンツの再生を停止する。

ポータブルデバイス 6 は、停止後に再度再生／停止ボタンが押圧操作されたとき、CPU 53 の制御に基づいて停止した位置からコンテンツの再生を再開する。再生／停止ボタンが押圧操作により再生を停止して操作が加わることなく数秒間経過したとき、ポータブルデバイス 6 は、自動的に電源をオフして消費電力を低減する。

因みに、ポータブルデバイス 6 は、電源がオフになった後に再生／停止ボタンが押圧操作されたとき、前回の停止した位置からコンテンツを再生せず、1 曲目から再生する。

また、ポータブルデバイス 6 の CPU 53 は、LCD コントローラ 68 を制御して、表示部 67 に、再生モードの状態（例えば、リピート再生、イントロ再生など）、イコライザ調整（すなわち、音声信号の周波数帯域に対応した利得の調整）、曲番号、演奏時間、再生、停止、早送り、早戻しなどの状態、音量及び乾電池 51 の残量等の情報を表示させる。

さらに、ポータブルデバイス 6 は、EEPROM 68 に、フラッシュメモリ 80 に書き込まれているコンテンツの数、それぞれのコンテンツが書き込まれているフラッシュメモリ 61 のブロック位置及びその他種々のメモリ蓄積情報等のいわゆる FAT（File Allocation Table）を格納する。

因みに、本実施の形態においては、コンテンツは、64 KByte を 1 ブロックとして扱われ、1 曲のコンテンツに対応したブロッ

ク位置がF A Tに格納される。

フラッシュメモリ 6 1 にF A Tが格納される場合、例えば、1 曲目のコンテンツがC P U 5 3 の制御によりフラッシュメモリ 6 1 に書き込まれると、1 曲目のコンテンツに対応するブロック位置がF A Tとしてフラッシュメモリ 6 1 に書き込まれ、次に、2 曲目のコンテンツがフラッシュメモリ 6 1 に書き込まれると、2 曲目のコンテンツに対応するブロック位置がF A Tとしてフラッシュメモリ 6 1（1 曲目と同一の領域）に書き込まれる。

このように、F A Tは、フラッシュメモリ 6 1 へのコンテンツの書き込みのたびに書き換えられ、更に、データの保護の為、同一のデータがリザーブ用に2 重に書き込まれる。

F A Tがフラッシュメモリ 6 1 に書き込まれると、1 回のコンテンツの書き込みに対応して、フラッシュメモリ 6 1 の同一の領域が2 回書き換えられるので、少ないコンテンツの書き込みの回数で、フラッシュメモリ 6 1 に規定されている書換えの回数に達してしまい、フラッシュメモリ 6 1 の書換えができなくなってしまう。

そこで、ポータブルデバイス 6 は、F A TをE E P R O M 6 8 に記憶させて、1 回のコンテンツの書き込みに対応するフラッシュメモリ 6 1 の書換えの頻度を少なくしている。

書換えの回数の多いF A TをE E P R O M 6 8 に記憶させることにより、F A Tをフラッシュメモリ 6 1 に記憶させる場合に比較して、ポータブルデバイス 6 は、コンテンツの書き込みができる回数を数十倍以上に増やすことができる。更に、C P U 5 3 は、E E P R O M 6 8 にF A Tを追記するように書き込ませるので、E E P R O M 6 8 の同一の領域の書換えの頻度を少なくして、E E P R O M

68が短期間で書換え不能になることを防止する。

ポータブルデバイス6は、USBケーブル7を介してパーソナルコンピュータ1に接続されたとき（以下、これをUSB接続と称する）、USBコントローラ57からCPU53に供給される割り込み信号に基づき、USB接続されたことを認識する。

ポータブルデバイス6は、USB接続されたことを認識すると、パーソナルコンピュータ1からUSBケーブル7を介して規定電流値の外部電力の供給を受けるとともに、電源回路52を制御して、乾電池51からの電力の供給を停止させる。

CPU53は、USB接続されたとき、DSP59のコンテンツの再生の処理を停止させる。これにより、CPU53は、パーソナルコンピュータ1から供給される外部電力が規定電流値を超えてしまうことを防止して、規定電流値の外部電力を常時受けられるように制御する。

このようにCPU53は、USB接続されると、乾電池51から供給される電力からパーソナルコンピュータ1から供給される電力に切り換えるので、電力単価の安いパーソナルコンピュータ1からの外部電力が使用され、電力単価の高い乾電池51の消費電力が低減され、かくして乾電池51の寿命を延ばすことができる。

なお、CPU53は、パーソナルコンピュータ1からUSBケーブル7を介して外部電力の供給を受けたとき、DSP59の再生処理を停止させることにより、DSP59からの輻射を低減させ、その結果としてパーソナルコンピュータ1を含むシステム全体の輻射を一段と低減させる。

つぎに、パーソナルコンピュータ1にインストールされたプログ

ラムの実行等により実現されるパーソナルコンピュータ 1 の機能について説明する。

図 4 は、所定のプログラムの実行等により実現される、パーソナルコンピュータ 1 の機能の構成を示す図である。

コンテンツ管理プログラム 1 1 1 は、EMD 選択プログラム 1 3 1、チェックイン／チェックアウト管理プログラム 1 3 2、コピー管理プログラム 1 3 3、移動管理プログラム 1 3 4、暗号方式変換プログラム 1 3 5、圧縮方式変換プログラム 1 3 6、暗号化プログラム 1 3 7、利用条件変換プログラム 1 3 9、利用条件管理プログラム 1 4 0、認証プログラム 1 4 1、復号プログラム 1 4 2、PD 用ドライバ 1 4 3、購入用プログラム 1 4 4 及び購入用プログラム 1 4 5 などの複数のプログラムで構成されている。

コンテンツ管理プログラム 1 1 1 は、例えば、シャッフルされているインストラクション、又は暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、コンテンツ管理プログラム 1 1 1 を読み出しても、インストラクションを特定できないなど）ように構成されている。

EMD 選択プログラム 1 3 1 は、コンテンツ管理プログラム 1 1 1 がパーソナルコンピュータ 1 にインストールされるとき、コンテンツ管理プログラム 1 1 1 には含まれず、EMD の登録の際に、ネットワーク 2 を介して、EMD 登録サーバ 3 から受信される。EMD 選択プログラム 1 3 1 は、EMD サーバ 4（4-1、4-2、4-3）のとの接続を選択して、購入用アプリケーション 1 1 5、又は購入用プログラム 1 4 4、1 4 5 に、EMD サーバ 4（4-1、

4-2, 4-3) との通信 (例えば、コンテンツを購入するときの、コンテンツのダウンロードなど) を実行させる。

チェックイン/チェックアウト管理プログラム 132 は、チェックイン又はチェックアウトの設定、及びコンテンツデータベース 114 に記録されている利用条件ファイル 162-1 ~ 162-N に基づいて、コンテンツファイル 161-1 ~ 161-N に格納されているコンテンツをポータブルデバイス 6 にチェックアウトするか、又はポータブルデバイス 6 に記憶されているコンテンツをチェックインする。

チェックイン/チェックアウト管理プログラム 132 は、チェックイン又はチェックアウトの処理に対応して、コンテンツデータベース 114 に記録されている利用条件ファイル 162-1 ~ 162-N に格納されている利用条件情報を更新する。

コピー管理プログラム 133 は、コンテンツデータベース 114 に記録されている利用条件ファイル 162-1 ~ 162-N に基づいて、コンテンツファイル 161-1 ~ 161-N に格納されているコンテンツをポータブルデバイス 6 にコピーするか、又はポータブルデバイス 6 からコンテンツをコンテンツデータベース 114 にコピーする。

移動管理プログラム 134 は、コンテンツデータベース 114 に記録されている利用条件ファイル 162-1 ~ 162-N に基づいて、コンテンツファイル 161-1 ~ 161-N に格納されているコンテンツをポータブルデバイス 6 に移動するか、又はポータブルデバイス 6 からコンテンツをコンテンツデータベース 114 に移動する。

暗号方式変換プログラム 135 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 115 が EMD サーバ 4-1 から受信したコンテンツの暗号化の方式、購入用プログラム 144 が EMD サーバ 4-2 から受信したコンテンツの暗号化の方式を、コンテンツデータベース 114 が記録しているコンテンツファイル 161-1 ~ 161-N に格納されているコンテンツと同一の暗号化の方式に変換する。

圧縮方式変換プログラム 136 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 115 が EMD サーバ 4-1 から受信したコンテンツの圧縮の方式、購入用プログラム 144 が EMD サーバ 4-2 から受信したコンテンツの圧縮の方式を、コンテンツデータベース 114 が記録しているコンテンツファイル 161-1 ~ 161-N に格納されているコンテンツと同一の圧縮の方式に変換する。

暗号化プログラム 137 は、例えば CD から読み取られ、録音プログラム 113 から供給されたコンテンツ（暗号化されていない）を、コンテンツデータベース 114 が記録しているコンテンツファイル 161-1 ~ 161-N に格納されているコンテンツと同一の暗号化の方式で暗号化する。

圧縮／伸張プログラム 138 は、例えば CD から読み取られ、録音プログラム 113 から供給されたコンテンツ（圧縮されていない）を、コンテンツデータベース 114 が記録しているコンテンツファイル 161-1 ~ 161-N に格納されているコンテンツと同一の符号化の方式で符号化する。圧縮／伸張プログラム 138 は、符号化されているコンテンツを伸張（復号）する。

利用条件変換プログラム139は、ネットワーク2を介して、購入用アプリケーションプログラム115がEMDサーバ4-1から受信したコンテンツの利用条件情報（いわゆる、Usage Rule）、購入用プログラム144がEMDサーバ4-2から受信したコンテンツの利用条件情報を、コンテンツデータベース114が記録している利用条件ファイル162-1～162-Nに格納されている利用条件情報と同一のフォーマットに変換する。

利用条件管理プログラム140は、コンテンツのコピー、移動、チェックイン、又はチェックアウトの処理を実行する前に、コンテンツデータベース114に記録されている利用条件ファイル162-1～162-Nに格納されている利用条件情報に対応するハッシュ値を基に、利用条件情報の改竄を検出する。利用条件管理プログラム140は、コンテンツのコピー、移動、チェックイン、又はチェックアウトの処理に伴う、コンテンツデータベース114に記録されている利用条件ファイル162-1～162-Nに格納されている利用条件情報を更新に対応して、利用条件情報に対応するハッシュ値を更新する。

認証プログラム141は、コンテンツ管理プログラム111と購入用アプリケーションプログラム115との相互認証の処理及びコンテンツ管理プログラム111と購入用プログラム144との相互認証の処理を実行する。また、認証プログラム141は、EMDサーバ4-3と購入用プログラム145との相互認証の処理で利用される認証鍵を記憶している。

認証プログラム141が相互認証の処理で利用する認証鍵は、コンテンツ管理プログラム111がパーソナルコンピュータ1にイン

ストールされたとき、認証プログラム 1 4 1 に記憶されておらず、表示操作指示プログラム 1 1 2 により登録の処理が正常に実行されたとき、EMD登録サーバ 3 から供給され、認証プログラム 1 4 1 に記憶される。

復号プログラム 1 4 2 は、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 ~ 1 6 1 - N に格納されているコンテンツをパーソナルコンピュータ 1 が再生するとき、コンテンツを復号する。

PD用ドライバ 1 4 3 は、ポータブルデバイス 6 に所定のコンテンツをチェックアウトするとき、又はポータブルデバイスから所定のコンテンツをチェックインするとき、ポータブルデバイス 6 にコンテンツ又はポータブルデバイス 6 に所定の処理を実行させるコマンドを供給する。

購入用プログラム 1 4 4 は、コンテンツ管理プログラム 1 1 1 とともにインストールされ、EMD登録サーバ 3 からネットワーク 2 を介して供給され、又は所定のCDに記録されて供給される。購入用プログラム 1 4 4 は、パーソナルコンピュータ 1 にインストールされたとき、コンテンツ管理プログラム 1 1 1 の有する所定の形式のインターフェースを介して、コンテンツ管理プログラム 1 1 1 とデータを送受信する。

購入用プログラム 1 4 4 は、例えば、シャッフルされているインストラクション、又は暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、購入用プログラム 1 4 4 を読み出しても、インストラクションを特定できないなど）ように

構成されている。

購入用プログラム 144 は、ネットワーク 2 を介して、EMD サーバ 4-2 に所定のコンテンツの送信を要求するとともに、EMD サーバ 4-2 からコンテンツを受信する。また、購入用プログラム 144 は、EMD サーバ 4-2 からコンテンツを受信するとき、課金の処理を実行する。

購入用プログラム 145 は、コンテンツ管理プログラム 111 とともにインストールされるプログラムであり、ネットワーク 2 を介して、EMD サーバ 4-3 に所定のコンテンツの送信を要求するとともに、EMD サーバ 4-3 からコンテンツを受信する。また、購入用プログラム 145 は、EMD サーバ 4-3 からコンテンツを受信するとき、課金の処理を実行する。

表示操作指示プログラム 112 は、フィルタリングデータファイル 181、表示データファイル 182、画像ファイル 183-1 ~ 183-K、又は履歴データファイル 184 を基に、ディスプレイ 20 に所定のウィンドウの画像を表示させ、キーボード 18 又はマウス 19 への操作を基に、コンテンツ管理プログラム 111 にチェックイン又はチェックアウトなどの処理の実行を指示する。

フィルタリングデータファイル 181 は、コンテンツデータベース 114 に記録されているコンテンツファイル 161-1 ~ 161-N に格納されているコンテンツそれぞれに重み付けをするためのデータを格納して、HDD 21 に記録されている。

表示データファイル 182 は、コンテンツデータベース 114 に記録されているコンテンツファイル 161-1 ~ 161-N に格納されているコンテンツに対応するデータを格納して、HDD 21 に

記録されている。

画像ファイル 183-1 ~ 183-K は、コンテンツデータベース 114 に記録されているコンテンツファイル 161-1 ~ 161-N に対応する画像、又は後述するパッケージに対応する画像を格納して、HDD 21 に記録されている。

以下、画像ファイル 183-1 ~ 183-K を個々に区別する必要がないとき、単に、画像ファイル 183 と称する。

履歴データファイル 184 は、コンテンツデータベース 114 に記録されているコンテンツファイル 161-1 ~ 161-N に格納されているコンテンツがチェックアウトされた回数、チェックインされた回数、その日付などの履歴データを格納して、HDD 21 に記録されている。

表示操作指示プログラム 112 は、登録の処理のとき、ネットワーク 2 を介して、EMD 登録サーバ 3 に、予め記憶しているコンテンツ管理プログラム 111 の ID を送信するとともに、EMD 登録サーバ 3 から認証用鍵及び EMD 選択プログラム 131 を受信して、コンテンツ管理プログラム 111 に認証用鍵及び EMD 選択プログラム 131 を供給する。

録音プログラム 113 は、所定のウィンドウの画像を表示させて、キーボード 18 又はマウス 19 への操作を基に、ドライブ 22 に装着された光ディスク 42 である CD からコンテンツの録音時間などのデータを読み出す。

録音プログラム 113 は、CD に記録されているコンテンツの録音時間などを基に、ネットワーク 2 を介して、WWW サーバ 5-1 又は 5-2 に CD に対応するデータ（例えば、アルバム名、又はア

ーティスト名など)又はCDに記録されているコンテンツに対応するデータ(例えば、曲名など)の送信を要求するとともに、WWWサーバ5-1又は5-2からCDに対応するデータ又はCDに記録されているコンテンツに対応するデータを受信する。

録音プログラム113は、受信したCDに対応するデータ又はCDに記録されているコンテンツに対応するデータを、表示操作指示プログラム112に供給する。

また、録音の指示が入力されたとき、録音プログラム113は、ドライブ22に装着された光ディスク42であるCDからコンテンツを読み出して、コンテンツ管理プログラム111に出力する。

コンテンツデータベース114は、コンテンツ管理プログラム111から供給された所定の方式で圧縮され、所定の方式で暗号化されているコンテンツを、コンテンツファイル161-1~161-Nのいずれかに格納する(HDD21に記録する)。コンテンツデータベース114は、コンテンツファイル161-1~161-Nにそれぞれ格納されているコンテンツに対応する利用条件情報を、コンテンツが格納されているコンテンツファイル161-1~161-Nにそれぞれ対応する利用条件ファイル162-1~162-Nのいずれかに格納する(HDD21に記録する)。

コンテンツデータベース114は、コンテンツファイル161-1~161-N又は利用条件ファイル162-1~162-Nをレコードとして記録してもよい。

例えば、コンテンツファイル161-1に格納されているコンテンツに対応する利用条件情報は、利用条件ファイル162-1に格納されている。コンテンツファイル161-Nに格納されているコ

ンテンツに対応する利用条件情報は、利用条件ファイル162-Nに格納されている。

以下、コンテンツファイル161-1~161-Nを個々に区別する必要がないとき、単に、コンテンツファイル161と称する。以下、利用条件ファイル162-1~162-Nを個々に区別する必要がないとき、単に、利用条件ファイル162と称する。

購入用アプリケーションプログラム115は、EMD登録サーバ3からネットワーク2を介して供給され、又は所定のCD-ROMに記録されて供給される。購入用アプリケーションプログラム115は、ネットワーク2を介して、EMDサーバ4-1に所定のコンテンツの送信を要求するとともに、EMDサーバ4-1からコンテンツを受信して、コンテンツ管理プログラム111に供給する。また、購入用アプリケーションプログラム115は、EMDサーバ4-1からコンテンツを受信するとき、課金の処理を実行する。

次に、表示データファイル182に格納されているデータとコンテンツデータベースに格納されているコンテンツファイル161-1~161-Nとの対応付けについて説明する。

コンテンツファイル161-1~161-Nのいずれかに格納されているコンテンツは、所定のパッケージに属する。パッケージは、より詳細には、オリジナルパッケージ、マイセレクトパッケージ、又はフィルタリングパッケージのいずれかである。

オリジナルパッケージは、1以上のコンテンツが属し、EMDサーバ4におけるコンテンツの分類（例えば、いわゆるアルバムに対応する）、又は一枚のCDに対応する。コンテンツは、いずれかのオリジナルパッケージに属し、複数のオリジナルパッケージに属す

ることができない。また、コンテンツが属するオリジナルパッケージは、変更することができない。使用者は、オリジナルパッケージに対応する情報の一部を編集（情報の追加、又は追加した情報の変更）することができる。

マイセレクトパッケージは、使用者が任意に選択した1以上のコンテンツが属する。マイセレクトパッケージにいずれのコンテンツが属するかは、使用者が任意に編集することができる。コンテンツは、1以上のマイセレクトパッケージに同時に属することができる。また、コンテンツは、いずれのマイセレクトパッケージに属しなくともよい。

フィルタリングパッケージには、フィルタリングデータファイル181に格納されているフィルタリングデータを基に選択されたコンテンツが属する。フィルタリングデータは、EMDサーバ4又はWWWサーバ5などからネットワーク2を介して供給され、又は所定のCDに記録されて供給される。使用者は、フィルタリングデータファイル181に格納されているフィルタリングデータを編集することができる。

フィルタリングデータは、所定のコンテンツを選択する、又はコンテンツに対応する重みを算出する基準となる。例えば、今週のJ-POP（日本のポップス）ベストテンに対応するフィルタリングデータを利用すれば、パーソナルコンピュータ1は、今週の日本のポップス1位のコンテンツ～今週の日本のポップス10位のコンテンツを特定することができる。

フィルタリングデータファイル181は、例えば、過去1月間にチェックアウトされていた期間が長い順にコンテンツを選択するフ

フィルタリングデータ、過去半年間にチェックアウトされた回数が多いコンテンツを選択するフィルタリングデータ、又は曲名に”愛”の文字が含まれているコンテンツを選択するフィルタリングデータなどを含んでいる。

このようにフィルタリングパッケージのコンテンツは、コンテンツに対応するコンテンツ用表示データ 2 2 1 (コンテンツ用表示データ 2 2 1 に使用者が設定したデータを含む)、又は履歴データ 1 8 4 などと、フィルタリングデータとを対応させて選択される。

ドライバ 1 1 7 は、コンテンツ管理プログラム 1 1 1 などの制御の基に、音声入出力インターフェース 2 4 を駆動して、外部から供給されたデジタルデータであるコンテンツを入力してコンテンツ管理プログラム 1 1 1 に供給するか、若しくはコンテンツ管理プログラム 1 1 1 を介してコンテンツデータベース 1 1 4 から供給されたコンテンツをデジタルデータとして出力するか、又は、コンテンツ管理プログラム 1 1 1 を介してコンテンツデータベース 1 1 4 から供給されたコンテンツに対応するアナログ信号を出力する。

図 5 は、表示操作指示プログラム 1 1 2 を起動させたとき、操作指示プログラム 1 1 2 がディスプレイ 2 0 に表示させる表示操作指示ウィンドウの例を示す図である。

表示操作指示ウィンドウには、録音プログラム 1 1 3 を起動させるためのボタン 2 0 1、EMD 選択プログラム 1 3 1 を起動させるためのボタン 2 0 2、チェックイン又はチェックアウトの処理の設定を行うフィールドを表示させるためのボタン 2 0 3、マイセレクトパッケージを編集するためフィールドを表示させるためのボタン 2 0 4 等が配置されている。

ボタン 2 0 5 が選択されているとき、フィールド 2 1 1 には、オリジナルパッケージに対応するデータが表示される。ボタン 2 0 6 が選択されているとき、フィールド 2 1 1 には、マイセレクトパッケージに対応するデータが表示される。ボタン 2 0 7 が選択されているとき、フィールド 2 1 1 には、フィルタリングパッケージに対応するデータが表示される。

フィールド 2 1 1 に表示されるデータは、パッケージに関するデータであり、例えば、パッケージ名称、又はアーティスト名などである。

例えば、図 5 においては、パッケージ名称”ファースト”及びアーティスト名”A 太郎”、パッケージ名称”セカンド”及びアーティスト名”A 太郎”などがフィールド 2 1 1 に表示される。

フィールド 2 1 2 には、フィールド 2 1 1 で選択されているパッケージに属するコンテンツに対応するデータが表示される。フィールド 2 1 2 に表示されるデータは、例えば、曲名、演奏時間、又はチェックアウト可能回数などである。

例えば、図 5 においては、パッケージ名称”セカンド”に対応するパッケージが選択されているので、パッケージ名称”セカンド”に対応するパッケージに属するコンテンツに対応する曲名”南の酒場”及びチェックアウト可能回数（例えば、8 分音符の 1 つがチェックアウト 1 回に相当し、8 分音符が 2 つでチェックアウト 2 回を示す）、並びに曲名”北の墓場”及びチェックアウト可能回数（8 分音符が 1 つでチェックアウト 1 回を示す）などがフィールド 2 1 2 に表示される。

このように、フィールド 2 1 2 に表示されるチェックアウト可能

回数としての１つの８分音符は、対応するコンテンツが１回チェックアウトできることを示す。

フィールド２１２に表示されるチェックアウト可能回数としての休符は、対応するコンテンツがチェックアウトできない（チェックアウト可能回数が０である。（ただし、パーソナルコンピュータ１はそのコンテンツを再生することができる。））ことを示す。また、フィールド２１２に表示されるチェックアウト可能回数としてのト音記号は、対応するコンテンツのチェックアウトの回数に制限がない（何度でも、チェックアウトできる）ことを示している。

なお、チェックアウト可能回数は、図５に示すように所定の図形（例えば、円、星、月などでもよい）の数で表示するだけでなく、数字等で表示してもよい。

また、表示操作指示ウィンドウには、選択されているパッケージ又はコンテンツに対応付けられている画像等（図４の画像ファイル１８３－１～１８３－Ｋのいずれかに対応する）を表示させるフィールド２０８が配置されている。ボタン２０９は、選択されているコンテンツを再生する（コンテンツに対応する音声スピーカー４５に出力させる）とき、クリックされる。

ボタン２０５が選択され、フィールド２１１に、オリジナルパッケージに対応するデータが表示されている場合、フィールド２１２に表示されている所定のコンテンツの曲名を選択して、消去の操作をしたとき、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１に、選択されている曲名に対応する、コンテンツデータベース１１４に格納されている所定のコンテンツを消去させる。

録音プログラム１１３が表示させるウィンドウのボタン（後述す

るボタン 2 5 5) が選択されて (アクティブにされて) いる場合、CD から読み出したコンテンツがコンテンツデータベース 1 1 4 に記録されたとき、表示操作指示プログラム 1 1 2 は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス 6 に記憶されているコンテンツの曲名を表示するフィールド 2 1 3 を表示する。

録音プログラム 1 1 3 が表示させるウィンドウのボタンが選択されている場合、CD から読み出したコンテンツがコンテンツデータベース 1 1 4 に記録されたとき、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 に、コンテンツデータベース 1 1 4 に記録した、CD から読み出したコンテンツを予め指定されているポータブルデバイス 6 にチェックアウトさせる。

フィールド 2 1 3 にはコンテンツの曲名に対応させて、フィールド 2 1 3 の最も左に、そのコンテンツがパーソナルコンピュータ 1 にチェックインできるか否かを示す記号が表示される。例えば、フィールド 2 1 3 の最も左に位置する “○” は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ 1 にチェックインできる (すなわち、パーソナルコンピュータ 1 からチェックアウトされた) ことを示している。フィールド 2 1 3 の最も左に位置する

“×” は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ 1 にチェックインできない (すなわち、パーソナルコンピュータ 1 からチェックアウトされていない、例えば、他のパーソナルコンピュータからチェックアウトされた) ことを示している。

表示操作指示プログラム 1 1 2 が表示操作指示ウィンドウにフィールド 2 1 3 を表示させたとき、表示操作指示プログラム 1 1 2 は、表示操作指示ウィンドウに、予め指定されているポータブルデバイ

ス 6 に記憶されているコンテンツが属するポータブルパッケージ（ポータブルデバイス 6 に記憶されているコンテンツが属するパッケージ）の名称を表示するフィールド 2 1 4、フィールド 2 1 3 を閉じるためのボタン 2 1 0 及びチェックイン又はチェックアウトを実行させるボタン 2 1 5 を表示する。

更に、表示操作指示プログラム 1 1 2 が表示操作指示ウィンドウにフィールド 2 1 3 を表示させたとき、表示操作指示プログラム 1 1 2 は、表示操作指示ウィンドウに、フィールド 2 1 2 で選択された曲名に対応するコンテンツのチェックアウトを設定するボタン 2 1 6、フィールド 2 1 3 で選択された曲名に対応するコンテンツのチェックインを設定するボタン 2 1 7、フィールド 2 1 3 に表示されたコンテンツ名に対応する全てのコンテンツのチェックインを設定するボタン 2 1 8 及びチェックイン又はチェックアウトの設定を取り消すボタン 2 1 9 を配置させる。

ボタン 2 1 6 乃至 2 1 9 の操作によるチェックイン又はチェックアウトの設定だけでは、パーソナルコンピュータ 1 は、チェックイン又はチェックアウトの処理を実行しない。

ボタン 2 1 6 乃至 2 1 9 の操作によるチェックイン又はチェックアウトの設定をした後、ボタン 2 1 5 がクリックされたとき、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 にチェックイン又はチェックアウトの処理を実行させる。すなわち、ボタン 2 1 5 がクリックされたとき、表示操作指示プログラム 1 1 2 は、チェックイン又はチェックアウトの設定に基づき、コンテンツ管理プログラム 1 1 1 に、ポータブルデバイス 6 にコンテンツを送信させるか、又はチェックインに対応する所定のコマンド（例え

ば、ポータブルデバイス 6 が記憶している所定のコンテンツを消去させるコマンドなど）を送信させるとともに、送信したコンテンツ又はコマンドに対応する利用条件ファイル 1 6 2 に格納されている利用条件情報を更新させる。

チェックイン又はチェックアウトが実行されたとき、表示操作指示プログラム 1 1 2 は、送信したコンテンツ又は送信されたコマンドに対応して、履歴データファイル 1 8 4 に格納されている履歴データを更新する。履歴データは、チェックイン又はチェックアウトされたコンテンツを特定する情報、又はそのコンテンツがチェックイン又はチェックアウトされた日付、そのコンテンツがチェックアウトされたポータブルデバイス 6 の名称などから成る。

チェックイン又はチェックアウトの設定の処理は短時間で実行できるので、使用者は、チェックイン又はチェックアウトの処理の実行後の状態を迅速に知ることができ、時間のかかるチェックイン又はチェックアウトの処理の回数を減らして、チェックイン又はチェックアウトに必要な時間全体（設定及び実行を含む）を短くすることができる。

図 6 は、録音プログラム 1 1 3 がディスプレイ 2 0 に表示させるウィンドウの例を説明する図である。

例えば、WWWサーバ 5 - 2 から受信した CD の情報を基に、録音プログラム 1 1 3 は、フィールド 2 5 1 に、“アシンクロナイズド”などの CD のタイトルを表示する。WWWサーバ 5 - 2 から受信した CD の情報を基に、録音プログラム 1 1 3 は、フィールド 2 5 2 に、例えば、“クワイ”などのアーティスト名を表示する。

WWWサーバ 5 - 2 から受信した CD の情報を基に、録音プログ

ラム 1 1 3 は、フィールド 2 5 3 の曲名を表示する部分に、例えば、” ヒート” , ” プラネット” , ” ブラック” , ” ソウル” などの曲名を表示する。同様に、録音プログラム 1 1 3 は、フィールド 2 5 3 のアーティストを表示する部分に、例えば、” クワイ” などのアーティスト名を表示する。

録音プログラム 1 1 3 が所定の C D の情報を受信した後、録音プログラム 1 1 3 は、H D D 2 1 の所定のディレクトリに C D の情報を格納する。

ボタン 2 5 4 などがクリックされて、C D の情報の取得の指示を受けたとき、録音プログラム 1 1 3 は、始めに、H D D 2 1 の所定のディレクトリを検索する。録音プログラム 1 1 3 は、そのディレクトリに C D の情報が格納されているとき、図示せぬダイアログボックスを表示して、使用者にディレクトリに格納されている C D の情報を利用するか否かを選択させる。

録音プログラム 1 1 3 が表示させるウィンドウに配置されているコンテンツの録音の開始を指示するボタン 2 5 6 がクリックされたとき、録音プログラム 1 1 3 は、ドライブ 2 2 に格納されている C D からコンテンツを読み出して、C D から読み出したコンテンツを C D の情報とともにコンテンツ管理プログラム 1 1 1 に供給する。コンテンツ管理プログラム 1 1 1 の圧縮／伸張プログラム 1 3 8 は、録音プログラム 1 1 3 から供給されたコンテンツを所定の圧縮の方式で圧縮して、暗号化プログラム 1 3 7 は、圧縮されたコンテンツを、暗号化する。また、利用条件変換プログラム 1 3 9 は、圧縮され、暗号化されたコンテンツに対応する利用条件情報を生成する。

コンテンツ管理プログラム 1 1 1 は、圧縮され、暗号化されたコ

ンテンツを利用条件情報とともに、コンテンツデータベース 1 1 4 に供給する。

コンテンツデータベース 1 1 4 は、コンテンツ管理プログラム 1 1 1 から受信したコンテンツに対応するコンテンツファイル 1 6 1 及び利用条件ファイル 1 6 2 を生成して、コンテンツファイル 1 6 1 にコンテンツを格納するとともに、利用条件ファイル 1 6 2 に利用条件情報を格納する。

コンテンツ管理プログラム 1 1 1 は、コンテンツデータベース 1 1 4 にコンテンツ及びコンテンツに対応する利用条件情報が格納されたとき、録音プログラム 1 1 3 から受信した C D の情報及び利用条件情報を表示操作指示プログラム 1 1 2 に供給する。

表示操作指示プログラム 1 1 2 は、録音の処理でコンテンツデータベース 1 1 4 に格納されたコンテンツに対応する利用条件情報及び C D の情報を基に、表示データファイル 1 8 2 に格納する表示用のデータを生成する。

録音プログラム 1 1 3 が表示させるウィンドウには、更に、C D から読み出したコンテンツをコンテンツデータベース 1 1 4 に記録したとき、自動的に、C D から読み出したコンテンツをポータブルデバイス 6 にチェックアウトさせるか否かの設定を行うボタン 2 5 5 が配置されている。

例えば、ボタン 2 5 5 がクリックされたとき、録音プログラム 1 1 3 は、ポータブルデバイス 6 を示すプルダウンメニューを表示する。使用者が、そのプルダウンメニューからポータブルデバイス 6 の選択をしたとき、選択されたポータブルデバイス 6 に自動的に、C D から記録したコンテンツをチェックアウトする。使用者が、そ

のプルダウンメニューから”チェックアウトしない”を選択した場合、パーソナルコンピュータ 1 は、CD からコンテンツを記録したとき、チェックアウトしない。

このように、録音プログラム 1 1 3 が表示させるウィンドウのボタン 2 5 5 をアクティブにしておくだけで、CD から読み出したコンテンツがコンテンツデータベース 1 1 4 に記録されたとき、パーソナルコンピュータ 1 は、予め指定されているポータブルデバイス 6 に、CD から読み出したコンテンツをチェックアウトさせることができる。

(2) 異なるフォーマット間での取り扱い

ところで、音楽コンテンツを提供するコンテンツ配信業者は、数多く存在し、それぞれの配信業者毎に、そのコンテンツの暗号化方式や圧縮方式、さらに、利用条件情報のフォーマットが異なっている。従って、一般にユーザは、提供を受けたいコンテンツの配信業者毎に、再生やチェックイン／チェックアウト用のコンテンツ管理アプリケーションやポータブルデバイスを購入しなければならなかった。そのため、ユーザは、1 つのパーソナルコンピュータ上に格納されている音楽コンテンツを、1 つの管理アプリケーションやポータブルデバイスで取り扱うことができなかった。

そこで、本システムでは、このように配信業者毎にフォーマットが異なるコンテンツを、パーソナルコンピュータ 1 上で統一的に取り扱っている。

以下、この音楽コンテンツ配信システムにおける、配信業者毎にフォーマットが異なるコンテンツの統一的な取り扱いについて、図 7 を参照して説明する。

ネットワーク 2 に接続された複数の EMD サーバは、例えば音楽提供会社 A から提供される音楽コンテンツを配信する EMD サーバ (A) 4-1、音楽提供会社 B から提供される音楽コンテンツを配信する EMD サーバ (B) 4-2、音楽提供会社 X から提供される音楽コンテンツを配信する EMD サーバ (X) 4-3 であるものとする。各 EMD サーバ 4 (4-1, 4-2, 4-3) は、各社独自にラインナップがされた音楽コンテンツを、ユーザが持つパーソナルコンピュータ 1 にネットワーク 2 を介して提供を行う。また、各 EMD サーバ 4 (4-1, 4-2, 4-3) では、音楽コンテンツの暗号化方式、利用条件 (Usage Rule) 情報のフォーマット、音楽コンテンツの圧縮方式、音楽コンテンツの課金方式等が各社独自の方式が採用されそれぞれ異なる方式により音楽コンテンツを配信している。

パーソナルコンピュータ 1 には、音楽コンテンツの再生や管理等を行うためのアプリケーションソフトウェアとして、EMD サーバ (A) 4-1 から音楽コンテンツの購入や管理や再生を行う再生用アプリケーション (A) 311 と、EMD サーバ (B) 4-2 から音楽コンテンツの購入や管理や再生を行う再生用アプリケーション (B) 312 と、音楽コンテンツをポータブルデバイス (A) 6-1 に転送するデバイスドライバ (A) 313 と、音楽コンテンツをポータブルデバイス (B) 6-2 に転送するデバイスドライバ (B) 314 とがインストールされている。なお、この図 7 で示す再生用アプリケーション 311, 312 は、図 4 で示した購入用アプリケーションプログラム 115 及びドライバ 117 に対応するものである。

また、パーソナルコンピュータ 1 には、HDD 2 1 内に格納されている全ての音楽コンテンツの包括的な管理を行う包括管理ユニット (X) 3 1 5 がインストールされている。この包括管理ユニット (X) 3 1 5 は、さらに、EMD 用受信インターフェース 3 1 6, EMD 用送信インターフェース 3 1 7, PD 用ドライバ 3 1 8 により構成されている。

また、ここでは、ポータブルデバイス (A) 6 - 1 は音楽提供会社 A に対応した専用の装置であり、ポータブルデバイス (B) 6 - 2 は音楽提供会社 B に対応した専用の装置であり、ポータブルデバイス (X) 6 - 3 は音楽提供会社 X に対応した専用の装置であるものとする。なお、ここでは、メモ리카ード内に格納した音楽コンテンツは、各音楽提供会社独自の暗号化方式で暗号化されており、また、その圧縮方式や利用条件情報のフォーマットも異なる。そのため、例えば他のデバイスドライバ等と直接接続して、音楽コンテンツを転送することはできないようになっているものとする。

再生用アプリケーション (A) 3 1 1 は、EMD サーバとの接続処理、ログファイル等をアップロードする処理、音楽コンテンツ、コンテンツ鍵及び利用条件情報等をダウンロードする処理等を行う。この再生用アプリケーション (A) 3 1 1 は、対応している EMD サーバに対してのみ接続処理を行うようになっている。ここでは、再生用アプリケーション (A) 3 1 1 は、EMD サーバ (A) 4 - 1 に対応した処理を行い、他の EMD サーバに対して接続処理を行うことができない。また、再生用アプリケーション (A) 3 1 1 は、EMD サーバ (A) 4 - 1 と接続した際の認証処理、ポータブルデバイス (A) 6 - 1 と接続した際の認証処理、HDD 2 1 に格納し

ている音楽コンテンツ及び利用条件情報の暗号化／暗号解読処理等を行う。再生用アプリケーション（A） 3 1 1 は、例えば、EMDサーバ（A） 4 - 1 からダウンロードした音楽コンテンツ及びその利用条件情報をコンテンツ鍵で暗号化し、このコンテンツ鍵をセッション鍵で暗号化して、HDD 2 1 に格納する。なお、暗号化処理の方式は、各再生用アプリケーションでそれぞれ独自の方式を採用している。そのため、パーソナルコンピュータ 1 内の同一のHDD 2 1 に格納されている音楽コンテンツであっても、専用の再生用アプリケーションでなければ、他の再生用アプリケーションでは暗号を解読することができないようになっている。

また、再生用アプリケーション（A） 3 1 1 は、各音楽コンテンツに付加されている利用条件情報の管理も行う。例えば、再生用アプリケーション（A） 3 1 1 は、利用条件情報に再生回数限度値が記述され、コンテンツの再生回数の制限がされている場合には、再生や複製を行う度に、再生や複製の回数限度値を1回分デクリメントする等の処理を行う。

また、再生用アプリケーション（A） 3 1 1 は、自己がHDD 2 1 上に管理している音楽コンテンツ及び利用条件情報を、包括管理ユニット（X） 3 1 5 のEMD用受信インターフェース 3 1 6 に送信する。

再生用アプリケーション（B） 3 1 2 は、EMDサーバとの接続処理、ログファイル等をアップロードする処理、音楽コンテンツ、コンテンツ鍵及び利用条件情報等をダウンロードする処理等を行う。この再生用アプリケーション（B） 3 1 2 は、対応しているEMDサーバに対してのみ接続処理を行うようになっている。具体的には、

再生用アプリケーション (B) 312 は、EMDサーバ (B) 4-2 に対応した処理を行い、他の EMDサーバに対して接続処理を行うことができない。また、再生用アプリケーション (B) 312 は、EMDサーバ (B) 4-2 と接続した際の認証処理、ポータブルデバイス (B) 6-2 と接続した際の認証処理、HDD 21 に格納している音楽コンテンツ及び利用条件情報の暗号化／暗号解読処理等を行う。再生用アプリケーション (B) 312 は、例えば、EMDサーバ (B) 4-2 からダウンロードした音楽コンテンツ及びその利用条件情報をコンテンツ鍵で暗号化し、このコンテンツ鍵をセッション鍵で暗号化して、HDD 21 に格納する。

また、再生用アプリケーション (B) 312 は、各音楽コンテンツに付加されている利用条件情報の管理も行う。例えば、再生用アプリケーション (B) 312 は、利用条件情報に再生回数限度値が記述され、コンテンツの再生回数の制限がされている場合には、再生や複製を行う度に、再生や複製の回数限度値を 1 回分デクリメントする等の処理を行う。

また、再生用アプリケーション (B) 312 は、自己が HDD 21 上に管理している音楽コンテンツ及び利用条件情報を、包括管理ユニット (X) 315 の EMD 用受信インターフェース 316 に送信する。

デバイスドライバ (A) 313 は、ポータブルデバイス (A) 6-1 への音楽コンテンツの転送等を行うアプリケーションソフトウェアである。デバイスドライバ (A) 313 は、ポータブルデバイス (A) 6-1 に音楽コンテンツを転送する。

デバイスドライバ (B) 314 は、ポータブルデバイス (B) 6

ー 2 への音楽コンテンツの転送等を行うアプリケーションソフトウェアである。デバイスドライバ (B) 3 1 4 は、ポータブルデバイス (B) 6 - 2 に音楽コンテンツを転送する。

包括管理ユニット (X) 3 1 5 は、EMD サーバ (X) 4 - 3 から音楽コンテンツの提供を受ける音楽提供会社 X 専用のアプリケーションソフトウェアであるとともに、デバイスドライバ (A) 3 1 3 及びデバイスドライバ (B) 3 1 4 や、再生用アプリケーション (A) 3 1 1 及び再生用アプリケーション (B) 3 1 2 との間で音楽コンテンツ及び利用条件情報の転送を行って、パーソナルコンピュータ 1 内の音楽コンテンツを包括的に管理を行う管理ソフトウェアでもある。また、自己が管理を行う音楽コンテンツを、携帯型の音楽再生装置である専用のポータブルデバイス (X) 6 - 3 に転送することができる。

なお、この包括管理ユニット (X) 1 1 5 は、図 4 に示したコンテンツ管理プログラム 1 1 1 に対応する処理を行う。

PD 用ドライバ 3 1 8 は、ポータブルデバイス (X) 6 - 3 との接続用のインターフェースモジュールで、このポータブルデバイス (X) 6 - 3 との間における認証処理や暗号化処理を行う。また、PD 用ドライバ 3 1 8 は、他のポータブルデバイス 8, 9 に音楽コンテンツ等を転送する場合には、デバイスドライバ (A) 3 1 3 やデバイスドライバ (B) 3 1 4 を介して音楽コンテンツ及び利用条件情報を転送する。

EMD 用受信インターフェース 3 1 6 は、再生用アプリケーション (A) 3 1 1 及び再生用アプリケーション (B) 3 1 2 からの音楽コンテンツ及び利用条件情報の受信、EMD サーバ (X) 4 - 3

からネットワーク 2 を介して転送された音楽コンテンツ及び利用条件情報の受信、及び、PD用ドライバ 318 との間での音楽コンテンツ及び利用条件情報の送受信を行う。

EMD用受信インターフェース 316 は、再生用アプリケーション (A) 311 及び再生用アプリケーション (B) 312 から音楽コンテンツ及び利用条件情報を受信する場合には、相互認証処理、暗号化方式の変換、転送する音楽コンテンツに付加された利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換等を行う。暗号化方式、利用条件情報、圧縮方式の変換は、再生用アプリケーション (A) 311 及び再生用アプリケーション (B) 312 が用いている方式から、包括管理ユニット (X) 315 が用いている方式に変換される。ここで包括管理ユニット (X) 315 が用いている方式を、以下、統一転送プロトコルと呼ぶ。そして、EMD用受信インターフェース 316 は、このように統一転送プロトコルに変換した音楽コンテンツ及び利用条件情報を、PD用ドライバ 318 を介してデバイスドライバ (A) 313 やデバイスドライバ (B) 314 に送信する。また、EMD用受信インターフェース 316 は、統一転送プロトコルに変換した音楽コンテンツ及び利用条件情報を、PD用ドライバ 318 を介して、ポータブルデバイス (X) 6-3 に送信する。

このように、EMDサーバ (A) 4-1 及びEMDサーバ (B) 4-2 から提供される音楽コンテンツは、一旦再生用アプリケーション (A) 311 及び再生用アプリケーション (B) 312 によりダウンロードされ、音楽コンテンツの暗号化方式、圧縮方式、利用条件情報が、統一転送プロトコルに変換されて、包括管理ユニット

(X) 315に転送される。包括管理ユニット(X) 315は、EMDサーバ(A) 4-1、EMDサーバ(B) 4-2)、EMDサーバ(X) 4-3からダウンロードされたそれぞれのコンテンツ提供会社の音楽コンテンツを統括的に管理を行うことができる。

また、EMD用受信インターフェース316は、音楽コンテンツの複製(コピー)、移動(ムーブ)、チェックイン、チェックアウトの機能を有している。

EMD用受信インターフェース316は、ユーザからの複製命令、移動命令に従い、例えば、再生用アプリケーション(A) 311や再生用アプリケーション(B) 312によって管理されている音楽コンテンツを、包括管理ユニット(X) 315に複製や移動する処理を行う。この際に、EMD用受信インターフェース316は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットの変換を行って、統一転送プロトコルとする。

また、ユーザからのCDリップング命令やチェックイン命令に従い、コンパクトディスク等の外部メディアやポータブルデバイス6(6-1, 6-2, 6-3)に格納されている音楽コンテンツを、包括管理ユニット(X) 315に複製やチェックインする処理を行う。この際に、EMD用受信インターフェース316は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットが統一転送プロトコルとされていなければ、これらの変換を行って、統一転送プロトコルとする。

また、ユーザからのチェックアウト命令に従い、包括管理ユニット(X) 315により管理されている音楽コンテンツを、ポータブルデバイス(X) 6-3に記録する処理を行う。この際に、EMD

用受信インターフェース 3 1 6 は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットが統一転送プロトコルとされていないければ、これらの変換を行って、統一転送プロトコルとする。また、この際に、利用条件のチェックアウト可能回数を 1 減少させる。

また、包括管理ユニット (X) 3 1 5 では、図 8 に示すように、アプリケーション層の下位レイヤに統一転送プロトコルを設けて、このレイヤにおいて他の再生用アプリケーションとのデータ転送を行っている。そして、包括管理ユニット (X) 3 1 5 は、この統一転送プロトコルの更に下位レイヤを `http` (`hyper Text Transfer Protocol`) として、EMDサーバ (X) 4 - 3 とのデータ送受信を行っている。

以上のような構成の音楽コンテンツ配信システムでは、EMDサーバ (A) 4 - 1 及び EMDサーバ (B) 4 - 2 から配信された音楽コンテンツを、包括管理ユニット (X) 3 1 5 が取得し、再生や管理を行うようになっている。そして、EMDサーバ (X) 4 - 3、EMDサーバ (A) 4 - 1 及び EMDサーバ (B) 4 - 2 から配信された音楽コンテンツを、ポータブルデバイス (X) 6 - 3 へ転送できるようになっている。

このように音楽コンテンツ配信システムでは、包括管理ユニット (X) 3 1 5 を中心として、各再生用アプリケーション及びデバイスドライバの間で、転送する音楽コンテンツの暗号化方式の変換、転送する音楽コンテンツに付加された利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換が行われ、統一転送プロトコルを用いて音楽コンテンツの転送が行われる。そのた

め、例えば、再生用アプリケーション（A） 3 1 1によりEMDサーバ（A） 4-1からダウンロードした音楽コンテンツ並びに再生用アプリケーション（B） 3 1 2によりEMDサーバB 4-2からダウンロードした音楽コンテンツを、包括管理ユニット（X） 3 1 5に転送することができる。このため、例えば音楽提供会社Aからのみ提供されるアーティストの音楽コンテンツを、ポータブルデバイス（X） 6-3に転送することができる。すなわち、この音楽コンテンツ配信システムでは、音楽コンテンツの暗号化方式、利用条件情報のフォーマット、音楽コンテンツの圧縮方式等を、統一転送プロトコルに変換するので、パーソナルコンピュータ1のハードディスク内に格納されている様々な方式の音楽コンテンツを、包括管理ユニット（X） 3 1 5やポータブルデバイス（X） 6-3により再生を行うことができる。特に、音楽コンテンツ配信システムでは、転送の際に、暗号化方式及び利用条件情報を変換するので、音楽コンテンツの著作権の保護を図りつつ、その音楽コンテンツの取り扱いの自由度を大きくすることができる。

すなわち、音楽コンテンツ配信システムでは、音楽コンテンツの再生や制御を行う再生用アプリケーション間で、少なくとも暗号化方式と利用条件情報の変換を行って、音楽コンテンツ及び利用条件情報の転送を行う。このことにより、音楽コンテンツ配信システムでは、複数の再生用アプリケーションが存在してもパーソナルコンピュータ1内の例えばHDD 21に格納されている音楽コンテンツを自由に移動させることができ、統一的な音楽コンテンツの管理をすることができる。また、音楽コンテンツとともに利用条件情報も転送するので、1つの音楽コンテンツに対して利用条件が重複した



りすることがなく、音楽コンテンツの著作権も確実に保護することができる。

(3) 利用条件情報

(一般的に用いられる利用条件情報の説明)

つぎに、再生用アプリケーション (A) 311 に用いられる利用条件情報のフォーマットの一例について説明をする。

再生用アプリケーション (A) 311 では、例えば、図 9 A に示すような表形式で記述された利用条件情報が用いられている。

表の左欄には、利用条件のポリシーが列方向に記述され、右欄には各ポリシーの具体的な値が記述される。例えば、ポリシーとして、再生開始可能日 (f r o m)、再生終了日 (t o)、1 回の再生に対する価格 (p a y / p l a y) 等が記述される。このような利用条件情報は、図 9 B に示すように各音楽コンテンツに付加された状態で、EMDサーバ (A) 4-1 から配信される。再生用アプリケーション (A) 311 は、記述されているポリシー及びその値に従い、音楽コンテンツの制御を行う。例えば、利用条件情報に、再生開始可能日 (f r o m) が 99 年 10 月 25 日、再生終了日 (t o) が 99 年 11 月 24 日、1 回の再生に対する価格 (p a y / p l a y) が y e s / 10 円と記述されているとする。この場合、その音楽コンテンツは、99 年 10 月 25 日から再生が可能とされ、それ以前にユーザから再生命令があっても、再生を禁止する。また、その音楽コンテンツは、99 年 11 月 24 日まで再生が可能とされ、それ以後となると、その音楽コンテンツを消去する。また、その音楽コンテンツは、1 回の再生の度に 10 円の課金を行うように設定されており、例えば、ユーザが再生した回数を別途ログ情報として

保管しておき、そのログ情報をEMDサーバ(A) 4-1にアップロードして、視聴したユーザに対して視聴した回数分だけの課金処理を行う。

(包括管理ユニットが用いている利用条件情報の説明)

つぎに、包括管理ユニット(X) 315が用いている利用条件情報について説明する。以下説明をする利用条件情報は、EMDサーバ(X) 4-3からダウンロードされる音楽コンテンツに付加されており、上記包括管理ユニット(X) 315がその音楽コンテンツの制御を行う際に用いられる。また、この利用条件情報は、再生用アプリケーション(A) 311と包括管理ユニット(X) 315との間、及び、再生用アプリケーション(B) 312と包括管理ユニット(X) 315との間で、音楽コンテンツの転送をする際の統一フォーマットとして用いられる。以下、この利用条件情報を、統一利用条件情報と称する。

統一利用条件情報は、図10に示すように、インデックスファイル331、オートマトンファイル332と、パラメータファイル333と、履歴ファイル334とから構成される。各ファイルは、XML(eXtensible Markup Language)言語で記述されている。

インデックスファイル331には、各ファイルのリファレンス情報等が記述されている。

オートマトンファイル332には、図11に示すように、利用条件がオートマトンで記述されたオートマトン記述部341と、コンテンツ鍵による認証コード(MAC:Message Authentication Code) 342、コンテンツ提供者の署名(Sig) 343、この署名を検証するための認証書(Cert) 344が付加されている。ここ

で、コンテンツ鍵を K_c 、コンテンツを作成したコンテンツ提供者のプライベート鍵及びパブリック鍵をそれぞれ K^{-1}_E , K^1_E とする。

オートマトン記述部 3 4 1 は、tuple 列で記述された Extended State Machine により音楽コンテンツの動作状態が記述される。

具体的には、オートマトン記述部 3 4 1 では、現在の音楽コンテンツの動作状態の集合を Q とし、音楽コンテンツのイベントを表す入力シンボルの集合を Σ とし、状態遷移した後の音楽コンテンツの動作状態の集合を Q' を以下のように表す。

$$Q' = \{ d \mid d = \delta(q, \alpha) \mid q \in Q, \alpha \in \Sigma, \delta : Q \times \Sigma \rightarrow Q \}$$

この式に示すように、状態遷移した後の状態 Q' の集合は、 d として表される。この d は、変数 q 、 α をもった関数 δ によって定義される。 q は、音楽コンテンツの動作状態の集合 Q のなかの 1 つの動作状態を示している。 α は、イベントの集合 Σ のなかの 1 つのイベントを示している。そして、関数 δ は、 Q 及び Σ のべき集合の Q への写像である。

そして、以上の Q , Σ , Q' に基づき、各 tuple を

$$\{ \langle q, \alpha, d \rangle \mid q, d \in Q, \alpha \in \Sigma \}$$

として表す。なお、 $\langle q, \alpha, d \rangle$ は、 q 、 α 、 d の順列のある組み合わせを示している。

ここで、 Σ には、再生 (Play), 複製 (copy), 支払い金額 (pay Y), 再生開始可能日時 (from YMD), 再生終了日時 (to YMD), 使用可能日数 (in Ddays), ヌルイベント (ϵ) といったイベントが、以下のように記述される。

$$\Sigma = \{ \text{Play, copy, pay } Y, \text{ from YMD, to YMD, in Ddays, } \epsilon \}$$

このようにオートマトン記述部 341 は、以上のように記述される。

このオートマトン記述部 341 への具体的な記述例について説明をする。

例えば、図 12 に示すような音楽コンテンツの動作遷移を示すオートマトンの tuple 列による記述例を、図 13 に示す。

このオートマトンは、以下に説明するような状態遷移をする。

まず、初期状態 q_0 から、状態 q_1 及び状態 q_5 に遷移する。状態 q_1 及び状態 q_5 以降は、それぞれ並行して動作する。

状態 q_1 で、所定金額（例えば 10 円）の支払いイベント（ $pay\ 10$ ）が発生すると状態 q_2 へ遷移する。状態 q_2 で、プレイイベント（ $play$ ）が発生すると状態 q_1 へ遷移する。すなわち、このオートマトンでは、10 円の支払いがされると、音楽コンテンツが 1 回だけ再生が可能となることを示している。また、状態 q_1 で、所定金額（例えば 1000 円）の支払いイベント（ $a.\ pay\ 1000$ ）が発生すると状態 q_3 へ遷移する。状態 q_3 では、プレイイベント（ $play$ ）が発生すると、再度この状態 q_3 に遷移する。すなわち、このオートマトンでは、1000 円の支払いがされると、音楽コンテンツが回数に制限無く再生が可能となることを示している。また、状態 q_1 で、一回の再生金額（例えば 10 円）の n 倍の金額の支払いイベント（ $pay\ 10 \times n$ ）が発生すると、状態 q_4 へ遷移する。状態 q_4 へ遷移してから、プレイイベント（ $play$ ）が発生すると、再度この状態 q_4 に遷移する。そして、この状態 q_4 で、 n 回のプレイイベントが発生すると、状態 q_1 に遷移する。すなわち、このオートマトンでは、 $10 \times n$ 円の支払いが

されると、音楽コンテンツが n 回再生が可能となることを示している。

また、状態 q_5 で、所定金額（例えば 100 円）の支払いイベント（ $pay\ 100$ ）が発生すると状態 q_6 へ遷移する。状態 q_6 で、コピーイベント（ $copy$ ）が発生すると状態 q_5 へ遷移する。また、状態 q_6 で、コピーイベント（ $copy$ ）が発生すると、状態 q_8 へ遷移する。状態 q_8 で、プレイイベント（ $play$ ）が発生すると、再度この状態 q_8 に遷移する。また、この状態 q_8 で、コピーイベント（ $copy$ ）が発生すると、状態 q_9 に遷移する。状態 q_9 では、どの状態へも遷移せずイベントも発生できない終端状態である。すなわち、このオートマトンでは、100 円の支払いがされると音楽コンテンツを他のデバイスへ 1 回コピーすることができることを示している。また、このオートマトンでは、コピーされた音楽コンテンツを再生することは何回でも可能であるが、他のデバイス等にコピーした場合には、再生ができなくなることを示している。

また、状態 q_5 で、所定金額（例えば 2000 円）の支払いイベント（ $a.\ pay\ 2000$ ）が発生すると状態 q_7 へ遷移する。状態 q_7 では、コピーイベント（ $copy$ ）が発生すると、再度この状態 q_7 に遷移する。また、状態 q_7 で、コピーイベント（ $copy$ ）が発生すると、状態 q_8 へ遷移する。状態 q_8 で、プレイイベント（ $play$ ）が発生すると、再度この状態 q_8 に遷移する。また、この状態 q_8 で、コピーイベント（ $copy$ ）が発生すると、状態 q_9 に遷移する。状態 q_9 では、どの状態へも遷移せずイベントも発生できない終端状態である。すなわち、このオートマトンで

は、2000円の支払いがされると、音楽コンテンツを他のデバイスへ回数制限無くコピーすることができることを示している。また、このオートマトンでは、コピーされた音楽コンテンツを再生することとは何回でも可能であるが、他のデバイス等にコピーした場合には、再生ができなくなることを示している。

そして、以上のように状態遷移をするオートマトンをtuple列で記述すると、図13に示すようになる。

また、オートマトン記述部341は、音楽コンテンツの動作を更新するため、動作状態の並列合成を記述しても良い。例えば、動作 a_0 と動作 a_1 との並列合成は、tuple列で以下のように表される。

$$\langle q_0, \alpha, a_0, q_0 \rangle$$

$$\langle q_0, \alpha, a_1, q_0 \rangle$$

また、オートマトン記述部341には、状態遷移に伴うアクションを記述してもよい。例えば、アクションは、tupleで以下のように表される。

$$\langle q_0, \alpha, q_1; action \rangle$$

このアクションは、予め定義した変数を用いた関数として表される。また、変数は、IDとスコープと初期値とからなる。スコープには、その音楽コンテンツ、アルバム、システム全体等のクラスがある。例えば、アルバム(a)の買い取りの値段を表す変数をnとし、 $a.n := 1000$ のように記述する。このように変数に対するアクションが記述されたオートマトン記述部341の一例を以下に示す。

$$\langle q_0, pay 100, q_1, a.n := a.n - 100 \rangle \dots (1)$$

$$\langle q_0, pay(a.n), q_1, a.n := 0 \rangle \dots (2)$$

$\langle q_1, \text{play}, q_2 \rangle \quad \dots (3)$

この例は、1つの音楽コンテンツの買い取り値段 {式(1)} が、アルバム買い取り {式(2)} の値段に影響を及ぼすことを示している。

以上のようなオートマトン記述部 341 は、図 14 に示すように、エントリー ID 345 と、コンテンツ ID 346 と、バージョン情報 347 と、変数情報 348 と、tuple 列 349 とから構成される。

以上のように記述フォーマットが定められたオートマトン記述部 341 の具体例について説明をする。

なお、以下にオートマトンの記述で用いられているイベント及びコマンドは、XML の仕様に基づいて規定された DTD (Document Type Definition) で定義されている。例えば、図 15 に示すように、再生動作 (play)、複製動作 (copy)、再生権購入 (pay-for-play)、複製権購入 (pay-for-copy)、アルバム再生権購入 (pay-for-album-play)、アルバム複製権購入 (pay-for-album-copy)、使用可能開始日 (from)、使用終了日 (to)、ヌル動作 (null) がイベントとして、DTD によって定義されている。

図 16 は、音楽コンテンツが 1999 年 9 月 1 日から再生が可能であることを示す XML 言語によるオートマトン記述部 341 の記述例である。

この図 16 に示す記述は、図 17 に示すようなオートマトンとなる。このオートマトンは、初期状態の状態 q_1 と、状態 q_2 とから構成される。状態 q_1 で、日付が使用可能開始日 (from) の 1999 年 9 月 1 日となると、状態 q_2 へ遷移する。そして、状態 q_2 で、再生イベント (play) が発生すると、音楽コンテンツの

再生を行い、再度状態 q 2 へ遷移する。このようにこのオートマトンは、音楽コンテンツを、1999年9月1日から再生を可能とするように制御している。

図18は、音楽コンテンツが1999年10月31日まで再生が可能であることを示すXML言語によるオートマトン記述部341の記述例である。

この図18に示す記述は、図19に示すようなオートマトンとなる。このオートマトンは、初期状態の状態 q 1 と、終端状態の状態 e n d とから構成される。状態2で、再生イベント (p l a y) が発生すると、音楽コンテンツの再生を行い、再度状態 q 2 へ遷移する。また、状態2で、使用終了日 (t o) の1999年10月31日となると、状態 e n d へ遷移する。状態 e n d となると、どの状態へも遷移せずイベントも発生しない。このように、このオートマトンは、音楽コンテンツを、1999年10月31日まで再生を可能とするように制御している。

図20は、音楽コンテンツの再生可能期間が1999年9月1日から1999年10月31日までであって、且つ、その再生可能回数が16回であることを示すXML言語によるオートマトン記述部341の記述例である。

この図20に示す記述は、図21に示すようなオートマトンとなる。このオートマトンは、初期状態の状態 q 1 と、状態 q 2 と、終端状態の状態 e n d とから構成される。状態 q 1 で、使用可能開始日 (f r o m) の1999年9月1日となると、状態 q 2 へ遷移する。そして、状態 q 2 で、再生イベント (p l a y) が発生すると、音楽コンテンツの再生を行い、再度状態 q 2 へ遷移する。また、状

態 2 で、使用終了日 (t o) の 1999 年 10 月 31 日となるか、
或いは、16 回再生イベント (p l a y × 16) が発生すると、状態 e n d へ遷移する。状態 e n d となると、どの状態へも遷移せずイベントも発生しない。このようにこのオートマトンは、音楽コンテンツの再生期間を 1999 年 9 月 1 日から 1999 年 10 月 31 日までとし、且つ、その再生回数を 16 回に制御している。

図 2 2 は、音楽コンテンツの再生回数を 16 回に制限することを示す XML 言語によるオートマトン記述部 3 4 1 の記述例である。

つぎに、パラメータファイル 3 3 3 には、図 2 3 に示すように、パラメータ記述部 3 5 1、コンテンツ鍵による認証コード 3 5 2、コンテンツ提供者の署名 3 5 3、この署名を検証するための認証書 3 5 4 が付加されている。ここで、コンテンツ鍵を K_c 、コンテンツを作成したコンテンツ提供者のプライベート鍵及びパブリック鍵をそれぞれ K^{-1}_E 、 K^1_E とする。

また、パラメータファイル 3 3 3 は、上記オートマトンファイル 3 3 2 を作成したコンテンツ提供者とは別のコンテンツ提供者（例えば、コンテンツ小売業者やコンテンツ中間業者等の二次提供者）により書き換えることが可能である。書き換えられたパラメータファイル 3 3 3 は、図 2 4 に示すように、それぞれの提供者や中間業者等に与えられたユニークなエンティティ ID 5 5 が付加される。ここで、 K'_c は、二次提供者のコンテンツ鍵で、 $K'_c = H(K_c, EntityID)$ となる。なお、ここで、 H は、一方向ハッシュ関数である。二次提供者のコンテンツ鍵 K'_c は、一次提供者のコンテンツ鍵 K_c から作成される。一次提供者と二次提供者とは、その認証書により区別される。

パラメータファイル 3 3 3 を検証する方法としては、コンテンツ鍵が得られていれば MAC により行い、安全性等の理由でコンテンツ鍵が得られない場合には署名と証明書により検証する。

MAC により検証するプロトコルは以下のようになる。コンテンツの一次提供者を S、二次提供者を A、端末を B とする。S → A は、S から A への伝送を示しており、S → B は、S から B への伝送を示しており、A → B は、A から B への伝送を示している。また、ID_A は、デバイス A の ID を示している。

S → A : $K'_c = H(K_c, ID_A)$

S → B : $X = E_K(K_c)$

A → B : $ID_A, \text{Parameters}, M = \text{MAC}_{K'_c}(\text{Parameters})$

B : $M \equiv \text{MAC}_{K'_c}(\text{Parameters}) ?$

このパラメータ記述部 3 5 1 には、上記オートマトンファイル 3 1 のオートマトン部 4 1 に記述された値の変更のための関数の係数が記述される。例えば、図 1 3 に示した例において、オートマトン部 4 1 では、例えば、以下のように音楽コンテンツの価格が関数となる場合がある。

$\langle q_0, \text{pay}(f_1(10)), q_1 \rangle$

$\langle q_1, \text{pay}(f_2(10) \times n), q_2 \rangle$

この場合、上記関数 f_1 及び f_2 を、例えば、以下のように定める。

$f_1(n) = 0.9n$

$f_2(n) = 90 + 0.1n$

このように関数を定めることによって、例えば、一次提供者が価格のデフォルト値を定め、二次提供者がパラメータファイル 3 3 3 を書き換えて、価格を変更することができる。

以上のようなパラメータ記述部 3 5 1 は、図 2 5 に示すように、エントリー ID 3 5 6 と、コンテンツ ID 3 5 7 と、係数情報 3 5 8 とから構成される。

履歴ファイル 3 3 4 は、オートマトン記述部 3 4 1 に記述内容に基づき動作する音楽コンテンツの動作の軌跡を記述するファイルである。この履歴ファイル 3 3 4 には、上記オートマトン記述 4 1 の `t u p l e` 内のステータスと変数を記録する。例えば、上述した図 1 3 に例において、2 回再生を行った場合には、

`< q 0 , q 1 , q 0 , q 1 >`

となり、これにより以下のような動作の軌跡を得ることができる。

`< p a y 1 0 , p l a y , p a y 1 0 , p l a y >`

これを集計して、例えば、包括管理ユニット (X) 3 1 5 にアップロード等すれば、ユーザの支払い金額を計算することができる。

以上のように音楽コンテンツ配信システムでは、ポリシー自体及びその具体的な値をプログラム化したオートマトンによって利用条件情報を記述しているので、コンテンツの利用条件の記載の自由度を高めることができる。

(4) 破壊された音楽コンテンツ等のリストア、再ダウンロード

つぎに、包括管理ユニット (X) 3 1 5 による音楽コンテンツのバックアップについて説明をする。

まず、包括管理ユニット (X) 3 1 5 の音楽コンテンツの鍵管理方法について、図 2 6 を用いて説明する。

包括管理ユニット (X) 3 1 5 は、パーソナルコンピュータ 1 内の HDD 2 1 に、音楽コンテンツ C 1 , C 2 , C 3 . . . C n を格納している。また、包括管理ユニット (X) 3 1 5 は、各音楽コン

テンツC 1, C 2, C 3 . . . C nに対応するコンテンツ鍵K c 1, K c 2, K c 3 . . . K c nも格納している。コンテンツ鍵K cは、音楽コンテンツCに対して一対一の関係となっている。また、各音楽コンテンツC 1, C 2, C 3 . . . C nには、それぞれの識別するためのコンテンツIDが付加されている。このコンテンツIDを、CID 1, CID 2, CID 3 . . . CID nとする。

音楽コンテンツC 1, C 2, C 3 . . . C nは、コンテンツ鍵K c 1, K c 2, K c 3 . . . K c nにより暗号化され、E (K c 1, C 1), E (K c 2, C 2), E (K c 3, C 3) . . . E (K c n, C n)とされた状態でパーソナルコンピュータ1のHDD 21内に記録されている。ここで、E (K, C)は、鍵KでコンテンツCを暗号化していることを示す。通常、コンテンツIDは、音楽コンテンツCのヘッダなどに記録されて音楽コンテンツCとともに暗号化されているか、或いは、MACが音楽コンテンツCに付加された状態とされており、音楽コンテンツ本体と切り離しができないようになっている。

また、コンテンツ鍵K c 1, K c 2, K c 3 . . . K c nは、ストレージ鍵K Sにより暗号化され、E (K S, K c 1), E (K S, K c 2), E (K S, K c 3) . . . E (K S, K c n)とされた状態でパーソナルコンピュータ1のHDD 21上に記録されている。このストレージ鍵K Sは、いわゆる耐タンパ性を有しており、通常のユーザからは参照することができない記録領域に保存されている。

以上のように鍵管理が行われる包括管理ユニット(X) 315では、例えば、音楽コンテンツC 1の再生を行う場合には、ストレージ鍵K Sを用いてコンテンツ鍵K c 1の暗号を解除し、続いて、こ

のコンテンツ鍵 $K_c 1$ を用いて、音楽コンテンツ $C 1$ の暗号を解除する。このことにより、包括管理ユニット $(X) 3 1 5$ は、音楽コンテンツ $C 1$ の再生を行うことができる。

また、以上のように鍵管理が行われる包括管理ユニット $(X) 3 1 5$ では、例えば、音楽コンテンツ $C 1$ をHDD $2 1$ からポータブルデバイス $(X) 6 - 3$ に移動(MOVE)する場合には、ポータブルデバイス $(X) 6 - 3$ との間で相互認証を行い、認証が完了するとストレージ鍵 K_S を用いてコンテンツ鍵 $K_c 1$ の暗号を解除し、続いて、セッション鍵によりコンテンツ鍵 $K_c 1$ を暗号化し、暗号化したコンテンツ鍵 $K_c 1$ 及び暗号化した音楽コンテンツ $C 1$ をポータブルデバイス $(X) 6 - 3$ に転送する。そして、コンテンツ鍵 $K_c 1$ と音楽コンテンツ $C 1$ とともにHDD $2 1$ から消去をする。このことにより、包括管理ユニット $(X) 3 1 5$ は、音楽コンテンツ $C 1$ をポータブルデバイス $(X) 6 - 3$ に移動することができる。

つぎに、HDD $2 1$ が破壊した場合など、音楽コンテンツやコンテンツ鍵をHDD $2 1$ から再生することができなくなったときにおける音楽コンテンツの復元方法について説明する。

まず、通常時において、包括管理ユニット $(X) 3 1 5$ は、暗号化した音楽コンテンツ C 及びコンテンツ鍵 K_c のバックアップデータを、HDD $2 1$ 内や他の記録媒体等に保存しておく。

また、通常時において、包括管理ユニット $(X) 3 1 5$ は、EMDサーバ $(X) 4 - 3$ からダウンロードした音楽コンテンツの購入記録と、HDD $2 1$ 内に記憶している全ての音楽コンテンツのコンテンツIDのリストとを、使用ログ情報として管理する。このログ情報は、音楽コンテンツをEMDサーバ $(X) 4 - 3$ からダウンロ

ードしたときや、ポータブルデバイス (X) 6-3 への移動等の音楽コンテンツの制御を行ったときに、更新するようにする。また、ログ情報は、HDD 21 の別領域や他の記録媒体に格納しておく。包括管理ユニット (X) 315 は、このログ情報を、定期的、或いは、アクセスした度に、EMDサーバ (X) 4-3 にアップロードする。

そして、包括管理ユニット (X) 315 の HDD 21 に格納されている音楽コンテンツ C やコンテンツ鍵 K_c が破壊されてしまった場合には、以下に示すような処理が行われる。

音楽コンテンツ C やコンテンツ鍵 K_c が破壊されてしまった場合、包括管理ユニット (X) 315 は、まず、EMDサーバ (X) 4-3 にアクセスを行って、ユーザ認証を行う。

続いて、EMDサーバ (X) 4-3 は、認証したユーザのユーザ ID から、包括管理ユニット (X) 315 の使用ログ情報を参照して、整合検証値 I C V (Integrity Check Value) を生成する。この整合検証値 I C V は、使用ログ情報に記述されている音楽コンテンツ C のコンテンツ ID である C I D と、包括管理ユニット (X) 315 のストレージ鍵 K S とに基づき、以下のように生成される。

$$I C V = H (K S, C I D 1 || C I D 2 || \dots || C I D n)$$

ここで、 $H (K, D a t a)$ は、一方向ハッシュ関数で、鍵 K によりその値が変化するものである。

続いて、EMDサーバ (X) 4-3 は、生成した整合検証値 I C V を、包括管理ユニット (X) 315 に送信する。

続いて、包括管理ユニット (X) 315 は、音楽コンテンツ C 又

はコンテンツ鍵K cがバックアップされていれば、そのバックアップデータをリストアして、音楽コンテンツC又はコンテンツ鍵K cをHDD 21内に保存する。また、音楽コンテンツC又はコンテンツ鍵K cがバックアップされていなければ、EMDサーバ(X) 4-3から破壊された音楽コンテンツC又はコンテンツ鍵K cを再配信してもらう。このとき、EMDサーバ(X) 4-3は、ユーザの購入履歴を参照して、以前に購入しているコンテンツであれば、課金処理を行わない。

包括管理ユニット(X) 315は、以上の処理を行い、破壊された音楽コンテンツC又はコンテンツ鍵K cを復活させる。

そして、包括管理ユニット(X) 315は、復活された音楽コンテンツC又はコンテンツ鍵K cの再生や制御を行う場合には、上記整合検証値ICVによりその音楽コンテンツのCIDをチェックするようにする。このように、整合検証値ICVを用いて復活させた音楽コンテンツC又はコンテンツ鍵K cをチェックすることにより、例えば、ある音楽コンテンツCiをポータブルデバイス(X) 6-3に移動してHDD 21上からは消去されている場合に、悪意のあるユーザが暗号化された音楽コンテンツCiであるE(Kci, Ci)を覚えておきリストアしたとしても、それらのデータは再生をすることもまた移動等の制御をすることもできない。

なお、音楽コンテンツC及びコンテンツ鍵K cではなく、ストレージ鍵KSが破壊されている場合には、包括管理ユニット(X) 315の再インストールを行う。この場合であっても、EMDサーバ(X) 4-3にユーザ登録をするとともにログ情報をアップロードしておけば、上述した方法でリストアや再ダウンロードをすること

ができる。

このように、音楽コンテンツ配信システムでは、例えば、ハードディスクのクラッシュ等により、音楽コンテンツが破壊されてしまった場合であっても、著作権を保護しながら、復元することができる。例えば、その音楽コンテンツが正規に購入したものであれば、無料で復活させることができる。

(5) 包括管理ユニットのマスター鍵及び認証鍵等の配布方法

包括管理ユニット (X) 315 とポータブルデバイス (X) 6-3 との間では、ポータブルデバイス (X) 6-3 の固有の ID 及び認証鍵 (MG-ID / IK) と、包括管理ユニット (X) 315 の固有のマスター鍵 (OMG-MK) とを用いて、相互認証が行われる。

包括管理ユニット (X) 315 とポータブルデバイス (X) 6-3 との間で、相互認証が行われると、包括管理ユニット (X) 315 からポータブルデバイス (X) 6-3 へ音楽コンテンツを送信 (チェックアウト) したり、ポータブルデバイス (X) 6-3 から包括管理ユニット (X) 315 への音楽コンテンツの返却 (チェックイン) をしたりできるようになる。なお、包括管理ユニット

(X) 315 は、パーソナルコンピュータ 1 の HDD 21 内に暗号化した音楽コンテンツを保存しており、また、ポータブルデバイス (X) 6-3 は、内部のメモ리카ード等の記憶媒体に暗号化した音楽コンテンツを保存する。そのため、包括管理ユニット (X) 315 からポータブルデバイス (X) 6-3 へ音楽コンテンツを送信する場合には、パーソナルコンピュータ 1 の HDD 21 上の音楽コンテンツが、ポータブルデバイス (X) 6-3 に装着されたメモ리카

ード上に転送されることとなる。また、ポータブルデバイス (X) 6-3 から包括管理ユニット (X) 3 1 5 へ音楽コンテンツを送信する場合には、ポータブルデバイス (X) 6-3 に装着されたメモ리카ード上の音楽コンテンツが、パーソナルコンピュータ 1 の HDD 2 1 上に転送されることとなる。

ポータブルデバイス (X) 6-3 は、ID 情報 (MG-ID)、複数世代分の認証鍵 (MG-IK) 及び複数世代分のマスター鍵 (OMG-MK) を工場出荷時から予め保持している。ポータブルデバイス (X) 6-3 には、後に外部からこれらの鍵等は供給されない。ポータブルデバイス (X) 6-3 は、必要に応じて、認証鍵 (MG-IK) 及びマスター鍵 (OMG-MK) の世代を更新する。ポータブルデバイス (X) 6-3 は、世代更新された最も新しい世代の認証鍵及びマスター鍵で相互認証を行い、旧世代の認証鍵及びマスター鍵では、相互認証を行わない。以下、ポータブルデバイス (X) 6-3 は、第 0 世代から第 99 世代の 100 世代分の認証鍵 (MG-IK [0-99]) 及びマスター鍵 (OMG-MK [0-99]) を保持しているものとする。なお、第 i 世代の認証鍵を (MG-IK [i]) と示し、第 i 世代のマスター鍵を (OMG-MK [i]) と示す。

また、包括管理ユニット (X) 3 1 5 は、マスター鍵 (OMG-MK) を保持することによって、オーディオ用コンパクトディスク等からパーソナルコンピュータ 1 内に音楽コンテンツを転送して、保存することができる。また、包括管理ユニット (X) 3 1 5 は、マスター鍵 (OMG-MK) を保持することによって、EMD サーバ (X) 4-3 から音楽コンテンツをダウンロードして、パーソナ

ルコンピュータ 1 内に保存することができる。

ここで、包括管理ユニット (X) 3 1 5 では、コンパクトディスクから音楽コンテンツを転送することはできるが EMD サーバ

(X) 4 - 3 からは音楽コンテンツをダウンロードすることができないマスター鍵 (OMG - MK) と、コンパクトディスクからも EMD サーバ (X) 4 - 3 からも音楽コンテンツを転送することができるマスター鍵 (OMG - MK) とが異なったものとなっている。

以下、コンパクトディスクから音楽コンテンツを転送することはできるが EMD サーバ (X) 4 - 3 からは音楽コンテンツをダウンロードすることができない鍵のことを、リッピング専用鍵ともいい、コンパクトディスクからも EMD サーバ (X) 4 - 3 からも音楽コンテンツを転送することができる鍵のことを EMD 鍵ともいう。

なお、本例では、第 0 世代のマスター鍵 (OMG - MK [0]) がリッピング専用鍵となっており、第 1 世代以後のマスター鍵 (OMG - MK [1 ~ 99]) が EMD 鍵となっている。

つぎに、リッピング専用鍵を用いた処理の手順について説明する。

包括管理ユニット (X) 3 1 5 が CD - ROM からインストールされる場合には、図 27 に示すように、包括管理ユニット (X) 3 1 5 のインストールソフトウェアが格納された CD - ROM 3 6 1 とともに、ポータブルデバイス (X) 6 - 3 と、フロッピーディスク 3 6 2 とが例えばセットで販売される。フロッピーディスク 3 6 2 には、ポータブルデバイス (X) 6 - 3 の ID 情報 (MG - ID), 第 0 世代の認証鍵 (MG - IK [0]), 第 0 世代のマスター鍵 (OMG - MK [0]) が格納されている。

続いて、販売されたポータブルデバイス (X) 6 - 3 等を使用可

能とするには、まず、CD-ROM 361をパーソナルコンピュータ1に装着する（ステップS11）。続いて、このCD-ROM 361から包括管理ユニット（X）315をパーソナルコンピュータ1にインストールする（ステップS12）。すると、包括管理ユニット（X）315がパーソナルコンピュータ1のハードディスク内に格納されることとなる（ステップS13）。続いて、フロッピーディスク362に格納されているポータブルデバイス（X）6-3のID情報（MG-ID）と、第0世代の認証鍵（MG-IK [0]）と、第0世代のマスター鍵（OMG-MK [0]）とをパーソナルコンピュータ1に保存する（ステップS14）。

このことによって、包括管理ユニット（X）315は、音楽CD 363等により提供される音楽コンテンツを、パーソナルコンピュータ1のハードディスク内に格納することができるようになる（ステップS15）。なお、第0世代のマスター鍵（OMG-MK [0]）は、リッピング専用鍵なので、EMDサーバ（X）4-3から音楽コンテンツをダウンロードできないようになっている。

また、ポータブルデバイス（X）6-3は、世代更新がされていく100世代分の認証鍵及びマスター鍵を内部に保持しているが、初期設定状態では、第0世代とされている。このため、第0世代の認証鍵及びマスター鍵を保持している包括管理ユニット（X）315と、ポータブルデバイス（X）6-3との相互認証が可能となる。したがって、音楽CD 363等により提供される音楽コンテンツを、ポータブルデバイス（X）6-3のメモリーカードに格納することができるようになる（ステップS16）。

一方、包括管理ユニット（X）315がネットワークを介して提

供される場合には、図 28 に示すように、ポータブルデバイス

(X) 6-3 とともに、インターネット上の EMD 登録サーバ 3 のアドレス、ユーザ ID 及びパスワード等が提供される。

続いて、販売されたポータブルデバイス (X) 6-3 等を使用可能とするには、まず、ユーザ ID 及びパスワードを用いてネットワーク上の EMD 登録サーバ 3 にアクセスをする (ステップ S 2 1)。続いて、EMD 登録サーバ 3 は、ユーザ ID 及びパスワードの認証を行う (ステップ S 2 2)。続いて、認証に問題がなければ、EMD 登録サーバ 3 は、包括管理ユニット (X) 3 1 5 のインストールソフトウェアと、ポータブルデバイス (X) 6-3 の ID 情報 (MG-ID) と、第 0 世代の認証鍵 (MG-IK [0]) と、第 0 世代のマスター鍵 (OMG-MK [0]) とを、パーソナルコンピュータ 1 に送信する (ステップ S 2 3)。続いて、パーソナルコンピュータ 1 は、包括管理ユニット (X) 3 1 5 のインストールソフトウェアを起動して、包括管理ユニット (X) 3 1 5 をインストールするとともに、ポータブルデバイス (X) 6-3 の ID 情報 (MG-ID) と、第 0 世代の認証鍵 (MG-IK [0]) と、第 0 世代のマスター鍵 (OMG-MK [0]) とを HDD 2 1 に保存する (ステップ S 2 4)。すると、ハードディスクには、包括管理ユニット (X) 3 1 5 が格納されることとなる (ステップ S 2 5)。

このことによって、包括管理ユニット (X) 3 1 5 は、音楽 CD 3 6 3 等により提供される音楽コンテンツを、パーソナルコンピュータ 1 の HDD 2 1 内に格納することができるようになる (ステップ S 2 6)。なお、第 0 世代のマスター鍵 (OMG-MK [0]) は、リッピング専用鍵なので、EMD サーバ (X) 4-3 から音楽

コンテンツをダウンロードできないようになっている。

また、ポータブルデバイス (X) 6-3 は、世代更新がされていく 100 世代分の認証鍵及びマスター鍵を内部に保持しているが、初期設定状態では、第 0 世代とされている。このため、第 0 世代の認証鍵及びマスター鍵を保持している包括管理ユニット (X) 315 と、ポータブルデバイス (X) 6-3 との相互認証が可能となる。したがって、音楽 CD 363 等により提供される音楽コンテンツを、ポータブルデバイス (X) 6-3 のメモ리카ード内に格納することができるようになる (ステップ S27)。

なお、以上の図 27 及び図 28 に示した方法に限られず、包括管理ユニット (X) 315 及びリッピング専用の第 0 世代のマスター鍵 (OMG-MK [0]) を CD-ROM 361 に格納しておき、ポータブルデバイス (X) 6-3 との認証用の ID 及び第 0 世代の認証鍵 (MG-ID / IK) をネットワークを介して提供しても良い。

つぎに、リッピング専用鍵を EMD 鍵に鍵に更新して、EMD サーバ (X) 4-3 からダウンロードした音楽コンテンツを取り扱えるようにする処理の手順について説明する。

包括管理ユニット (X) 315 は、図 27 又は図 28 に示した手順により、CD-ROM 等のリムーバブルメディアやインターネット等のネットワークを介して提供され、パーソナルコンピュータ 1 内の HDD 21 にインストールされている。このとき包括管理ユニット (X) 315 は、リッピング専用である第 0 世代のマスター鍵 (OMG-MK [0]) と、認証用の ID 及び第 0 世代の認証鍵 (MG-ID / IK [0]) とを保持しており、ポータブルデバイ

ス (X) 6-3 の鍵の世代もデフォルトのままである。

まず、パーソナルコンピュータ 1 は、図 29 に示すように、ユーザ ID 及びパスワードを用いてネットワーク上の EMD 登録サーバ 3 にアクセスをする (ステップ S 31)。続いて、EMD 登録サーバ 3 は、ユーザ ID 及びパスワードの認証を行う (ステップ S 32)。続いて、認証に問題がなければ、EMD 登録サーバ 3 は、パーソナルコンピュータ 1 の ID 情報 (OMG-ID) を登録し、包括管理ユニット (X) 315 が EMD サーバ (X) 4-3 と接続するための公開鍵 (OMG-PK)、秘密鍵 (OMG-KS) 及び公開鍵の認証書 (Cert [PK]) を生成する (ステップ S 33)。続いて、EMD 登録サーバ 3 は、生成した公開鍵 (OMG-PK)、秘密鍵 (OMG-KS) 及び公開鍵の認証書 (Cert [PK]) を、パーソナルコンピュータ 1 に送信する (ステップ S 34)。

続いて、EMD 登録サーバ 3 は、ポータブルデバイス (X) 6-3 の ID 情報 (MG-ID)、第 i 世代の認証鍵 (MG-IK [i])、第 i 世代のマスター鍵 (OMG-MK [i]) をパーソナルコンピュータ 1 に送信する (ステップ S 35)。続いて、パーソナルコンピュータ 1 の包括管理ユニット (X) 315 は、受信した ID 情報 (MG-ID)、第 i 世代の認証鍵 (MG-IK [i])、第 i 世代のマスター鍵 (OMG-MK [i]) に基づき、これらの鍵を第 i 世代に世代更新する (ステップ S 36)。続いて、包括管理ユニット (X) 315 は、ポータブルデバイス (X) 6-3 との間で認証を行う (ステップ S 37)。ポータブルデバイス (X) 6-3 は、認証がされると、自己の鍵の世代を第 i 世代に更新する (ステップ S 38)。

このことによって、包括管理ユニット (X) 315 は、音楽 CD 363 等により提供される音楽コンテンツを、パーソナルコンピュータ 1 のハードディスク内に格納するとともに、EMD サーバ (X) 4-3 からダウンロードした音楽コンテンツをパーソナルコンピュータ 1 の HDD 21 に格納することができるようになる。

つぎに、EMD 鍵等の世代更新をする手順について説明する。

包括管理ユニット (X) 315 は、第 i 世代のマスター鍵 (OMG-MK [i]) と、認証用の ID 及び第 0 世代の認証鍵 (MG-ID / IK [i]) とを保持しており、ポータブルデバイス (X) 6-3 の鍵の世代も第 i 世代となっている。

まず、図 30 に示すように、パーソナルコンピュータ 1 が何らかの処理のため、EMD 登録サーバ 3 にアクセスすると、EMD 登録サーバ 3 は、包括管理ユニット (X) 315 の ID を認証して、第 $(i+k)$ 世代の認証鍵 (MG-IK [$i+k$]) 及び第 $(i+k)$ 世代のマスター鍵 (OMG-MK [$i+k$]) をパーソナルコンピュータ 1 に送信する (ステップ S41)。続いて、パーソナルコンピュータ 1 の包括管理ユニット (X) 315 は、受信した認証鍵及びマスター鍵を、第 $(i+k)$ 世代に更新する (ステップ S42)。続いて、包括管理ユニット (X) 315 は、ポータブルデバイス (X) 6-3 と認証を行う (ステップ S43)。ポータブルデバイス (X) 6-3 は、認証がされると、自己の鍵の世代を第 i 世代から第 $(i+k)$ 世代に更新する (ステップ S44)。

また、図 31 に示すように、一方、ポータブルデバイス (X) 6-3 が用いている認証鍵等の世代が第 $(i+k)$ 世代となっており、

包括管理ユニット (X) 315 が保持している認証鍵等の世代が第 i 世代となっている場合には、ポータブルデバイス (X) 6-3 と包括管理ユニット (X) 315 との認証が行われると、認証失敗となる (ステップ S 51)。認証を失敗すると、包括管理ユニット

(X) 315 は、EMD 登録サーバ 3 に対して、鍵要求を行う (ステップ S 52)。鍵要求があると、EMD 登録サーバ 3 は、包括管理ユニット (X) 315 の ID を認証して、第 $(i+k)$ 世代の認証鍵 ($MG-IK[i+k]$) 及び第 $(i+k)$ 世代のマスター鍵 ($OMG-MK[i+k]$) を送信する (ステップ S 53)。続いて、包括管理ユニット (X) 315 は、受信した認証鍵及びマスター鍵を、第 $(i+k)$ 世代に更新する (ステップ S 54)。続いて、包括管理ユニット (X) 315 は、ポータブルデバイス (X) 6-3 と認証を行う (ステップ S 55)。

このことによって、包括管理ユニット (X) 315 は、音楽 CD 363 等により提供される音楽コンテンツを、パーソナルコンピュータ 1 のハードディスク内に格納するとともに、EMD サーバ (X) 4-3 からダウンロードした音楽コンテンツをパーソナルコンピュータ 1 の HDD 21 に格納することができるようになる (ステップ S 38)。

以上のように、音楽コンテンツ配信システムでは、包括管理ユニット (X) 315 及びポータブルデバイス (X) 6-3 が用いるマスター鍵及び認証鍵を、リッピング専用の鍵とサーバ接続鍵とに分け、さらに、サーバ接続鍵をネットワークを介してダウンロードするようにしている。このため、音楽コンテンツ配信システムでは、サーバから配信された音楽コンテンツの安全性が高まり、例えば、

リップリング専用の鍵が破られたとしても、サーバからダウンロードされる音楽コンテンツを破ることができない。

また、音楽コンテンツ配信システムでは、包括管理ユニット (X) 315 及びポータブルデバイス (X) 6-3 が用いるマスター鍵及び認証鍵を、世代更新させて用いている。さらに、包括管理ユニット (X) 315 は、マスター鍵及び認証鍵がネットワークを介して供給され、世代更新を行う。このため、音楽コンテンツの安全性が高まる。

産業上の利用可能性

本発明にかかるコンテンツ提供システム及びコンテンツ提供方法では、再生プログラムが、外部記憶媒体に格納されたコンテンツデータのみを取り扱う場合には、第1の認証鍵及び第1のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。再生プログラムが、ネットワークを介して提供されたコンテンツデータを取り扱う場合には、第1の認証鍵及び第1のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。第2の認証鍵及び第2のマスター鍵は、ネットワークを介して再生プログラムに提供され、第1の認証鍵及び第1のマスター鍵と異なる鍵となっている。

このことにより、本発明では、ネットワークを介して配信されたコンテンツデータの安全性を高めることができる。

請求の範囲

1. コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとからなるコンテンツ提供システムにおいて、

上記データ処理装置は、

上記再生プログラムがインストールされた後に、第1のマスター鍵及び第1の認証鍵が上記再生プログラムに提供され、上記第1のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第1の認証鍵及び第1のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、

上記再生プログラムが上記コンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第1のマスター鍵とは異なる第2のマスター鍵及び上記第1の認証鍵とは異なる第2の認証鍵がネットワークを介して提供され、この提供された第2のマスター鍵を用いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第2の認証鍵及び第2のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うこと

を特徴とするコンテンツ提供システム。

2. 上記可搬再生装置は、第1から第 i (i は2以上の整数) 世



代まで世代更新されていく第 1 から第 i の認証鍵、及び、第 1 から第 i (i は 2 以上の整数) 世代まで世代更新されていく第 1 から第 i のマスター鍵を保持しており、

上記再生プログラムは、第 2 から第 i (i は 2 以上の整数) まで世代更新されていく第 2 から第 i の認証鍵、及び、第 2 から第 i

(i は 2 以上の整数) まで世代更新されていく第 2 から第 i のマスター鍵がネットワークを介して提供され、

上記可搬再生装置と上記再生プログラムとは、同一世代の認証鍵を用いて相互認証を行うこと

を特徴とする請求の範囲第 1 項記載のコンテンツ提供システム。

3. 上記可搬再生装置は、上記再生プログラムと認証を行った際に、この再生プログラムが用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記再生プログラムが用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求の範囲第 2 項記載のコンテンツ提供システム。

4. 上記再生プログラムは、上記可搬再生装置と認証を行った際に、上記可搬再生装置が用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記コンテンツサーバに鍵要求をして、上記可搬再生装置が用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求の範囲第 2 項記載のコンテンツ提供システム。

5. 上記コンテンツサーバは、上記再生プログラムからアクセスされた際に、上記再生プログラムが用いている認証鍵の世代よりも新しい世代の認証鍵及びマスター鍵を上記再生プログラムに提供して、上記再生プログラムが用いている認証鍵の世代更新をすること

を特徴とする請求の範囲第2項記載のコンテンツ提供システム。

6. コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置とによりユーザにコンテンツデータを提供するコンテンツサーバとからなるコンテンツ提供方法において、

上記再生プログラムをインストールした後に、第1のマスター鍵及び第1の認証鍵が上記再生プログラムに提供され、上記第1のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第1の認証鍵及び第1のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、

上記再生プログラムがコンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第1のマスター鍵とは異なる第2のマスター鍵及び上記第1の認証鍵とは異なる第2の認証鍵がネットワークを介して提供され、この提供された第2のマスター鍵を用いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第2の認証鍵及び第2のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うこと

を特徴とするコンテンツ提供方法。

7. 上記可搬再生装置が、第1から第 i (i は2以上の整数)世代まで世代更新されていく第1から第 i の認証鍵、及び、第1から第 i (i は2以上の整数)世代まで世代更新されていく第1から第 i のマスター鍵を保持しており、



上記再生プログラムは、第2から第 i (i は2以上の整数)まで世代更新されていく第2から第 i の認証鍵、及び、第2から第 i (i は2以上の整数)まで世代更新されていく第2から第 i のマスター鍵がネットワークを介して提供され、

上記可搬再生装置と上記再生プログラムとは、同一世代の認証鍵を用いて相互認証を行うこと

を特徴とする請求の範囲第6項記載のコンテンツ提供方法。

8. 上記可搬再生装置が、上記再生プログラムと認証を行った際に、この再生プログラムが用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記再生プログラムが用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求の範囲第7項記載のコンテンツ提供方法。

9. 上記再生プログラムが、上記可搬再生装置と認証を行った際に、上記可搬再生装置が用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記コンテンツサーバに鍵要求をして、上記可搬再生装置が用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求の範囲第7項記載のコンテンツ提供方法。

10. 上記コンテンツサーバが、上記再生プログラムからアクセスされた際に、上記再生プログラムが用いている認証鍵の世代よりも新しい世代の認証鍵及びマスター鍵を上記再生プログラムに提供して、上記再生プログラムが用いている認証鍵の世代更新をすること

を特徴とする請求の範囲第7項記載のコンテンツ提供方法。

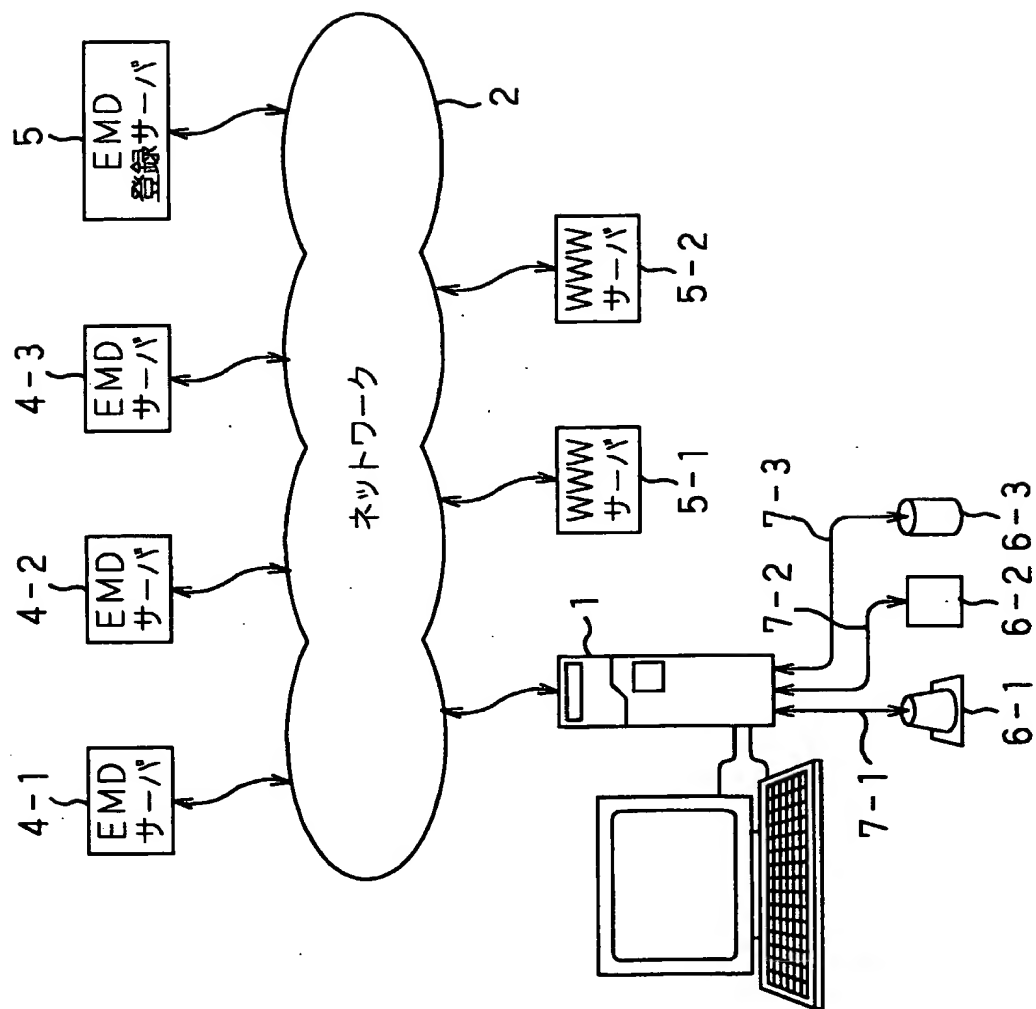


Fig.1

This Page Blank (uspto)

2/26

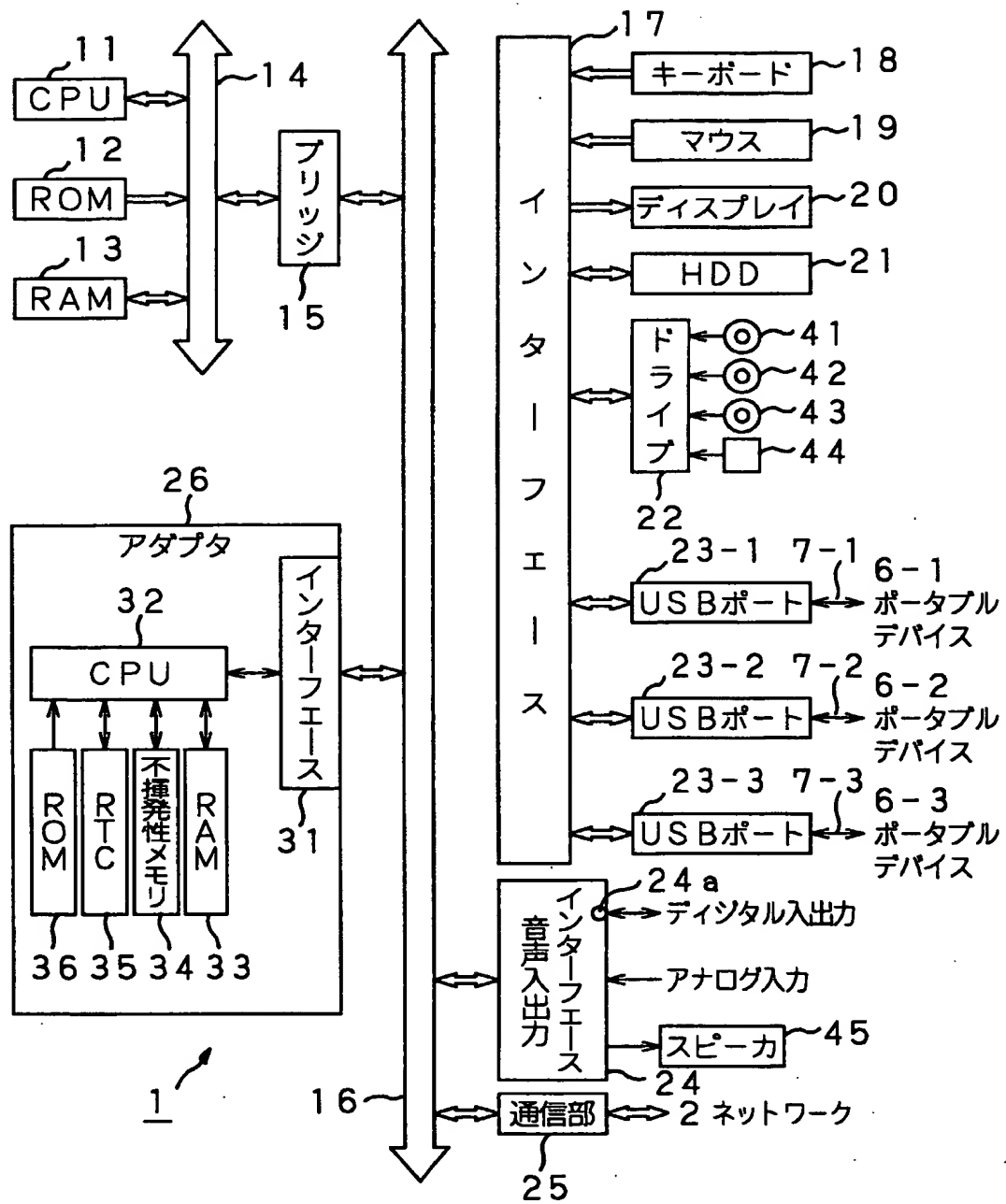


Fig. 2

This Page Blank (uspto)

3/26

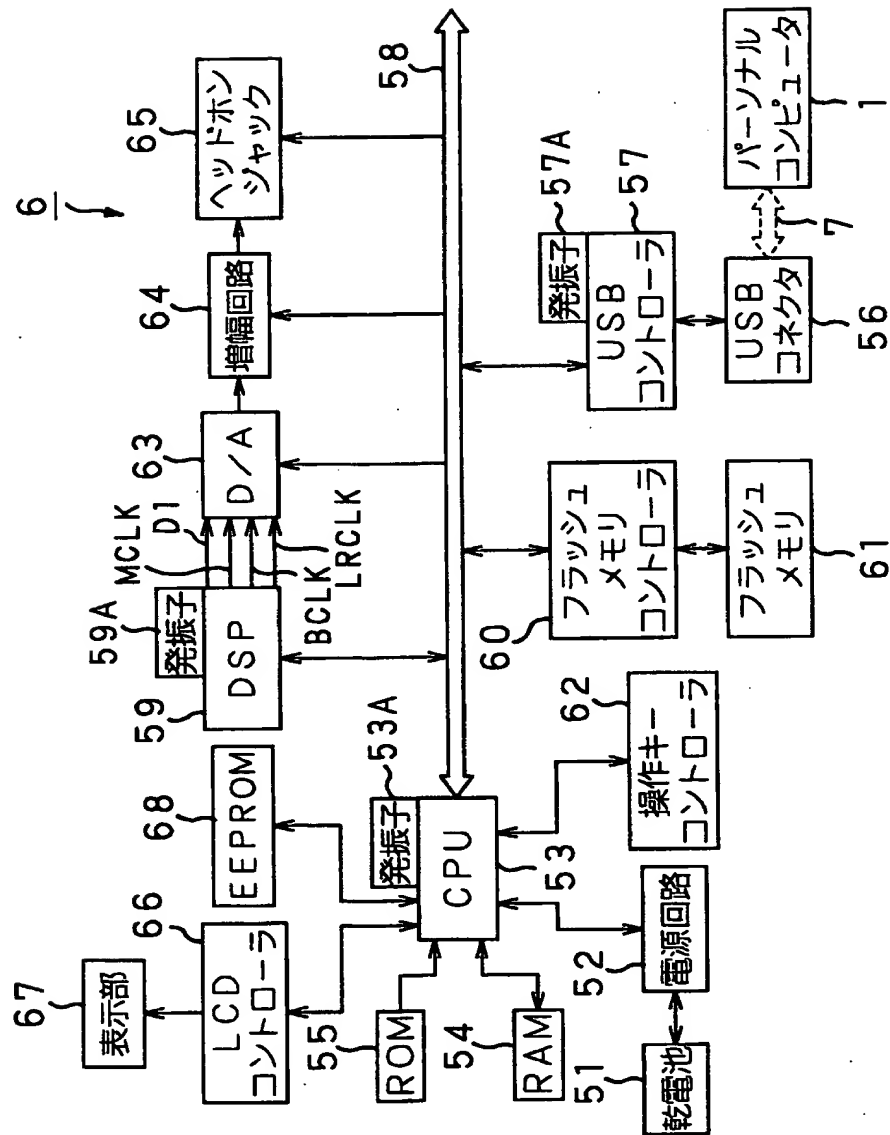


Fig. 3

This Page Blank (uspto)

4/26

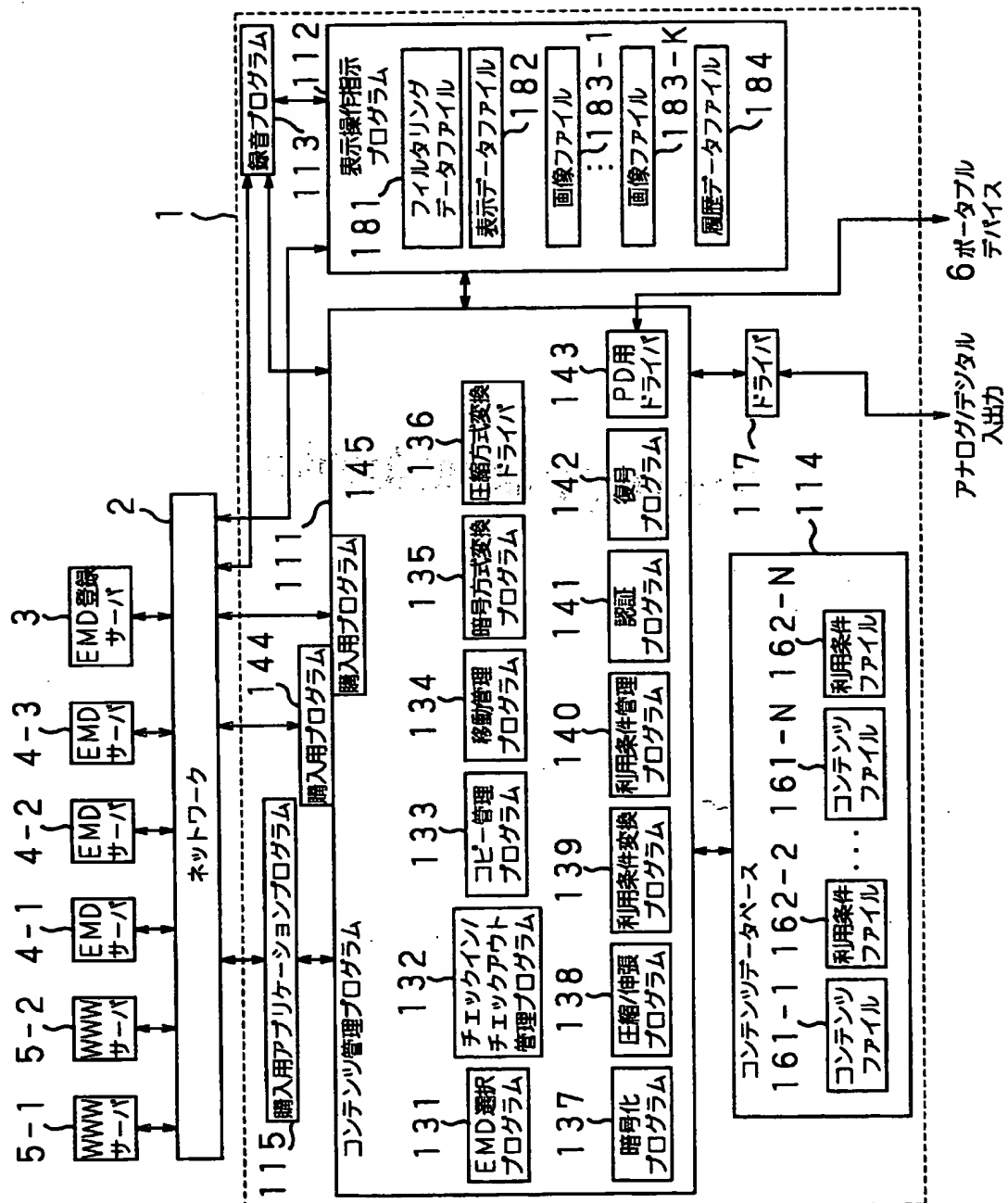


Fig. 4

This Page Blank (uspto)

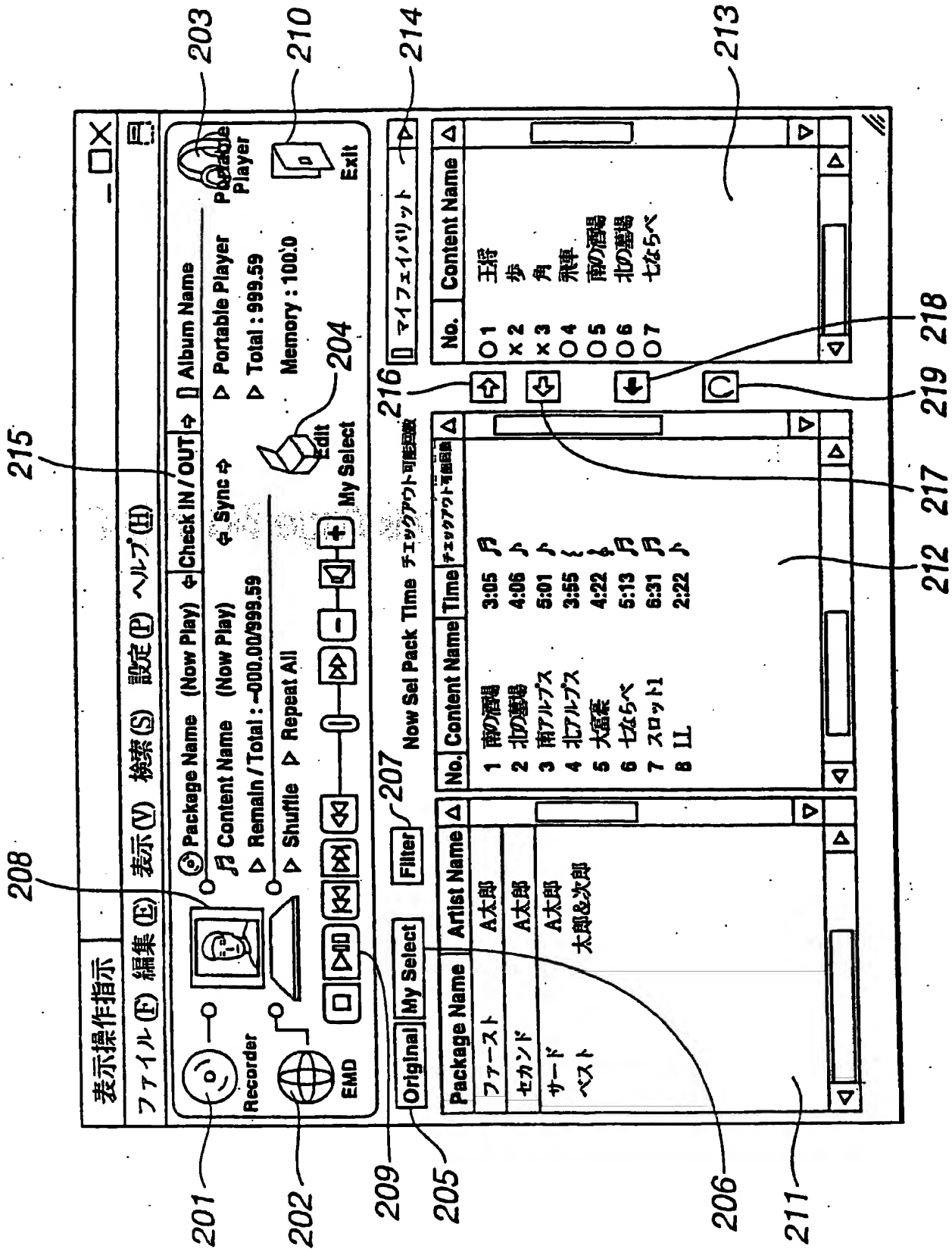
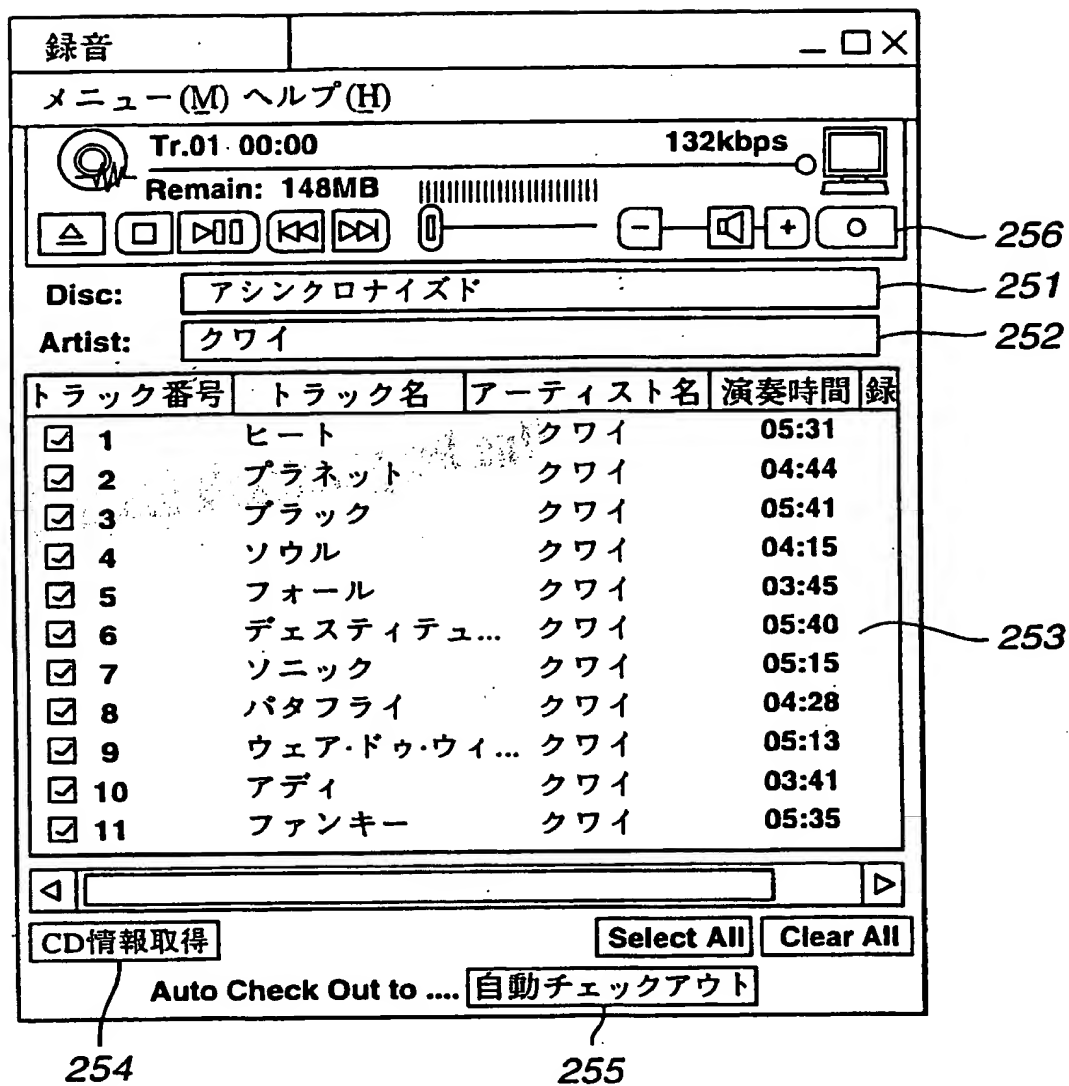


Fig. 5

This Page Blank (uspto)

6/26



Fi g.6

This Page Blank (uspto)

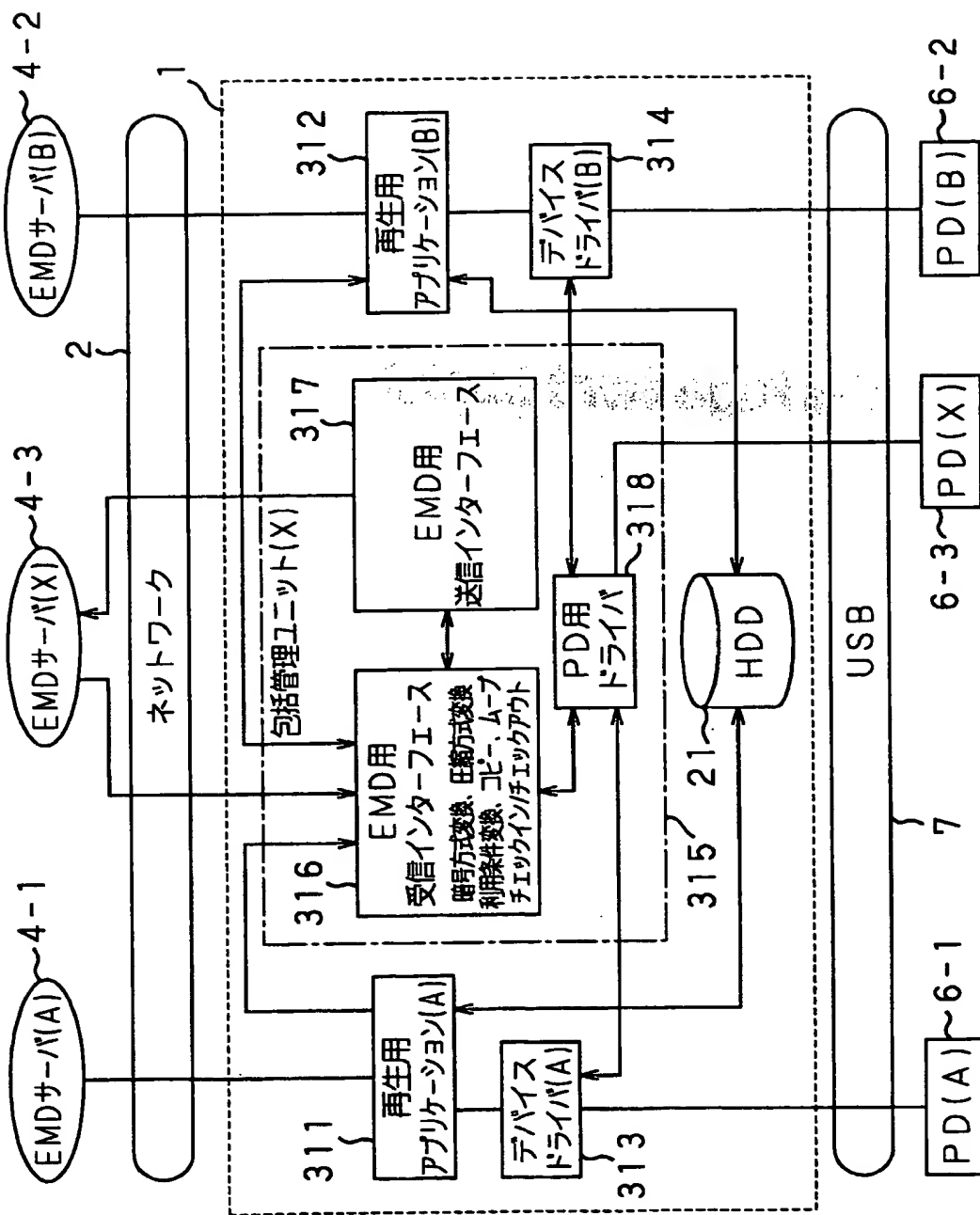


Fig. 7

This Page Blank (uspto)

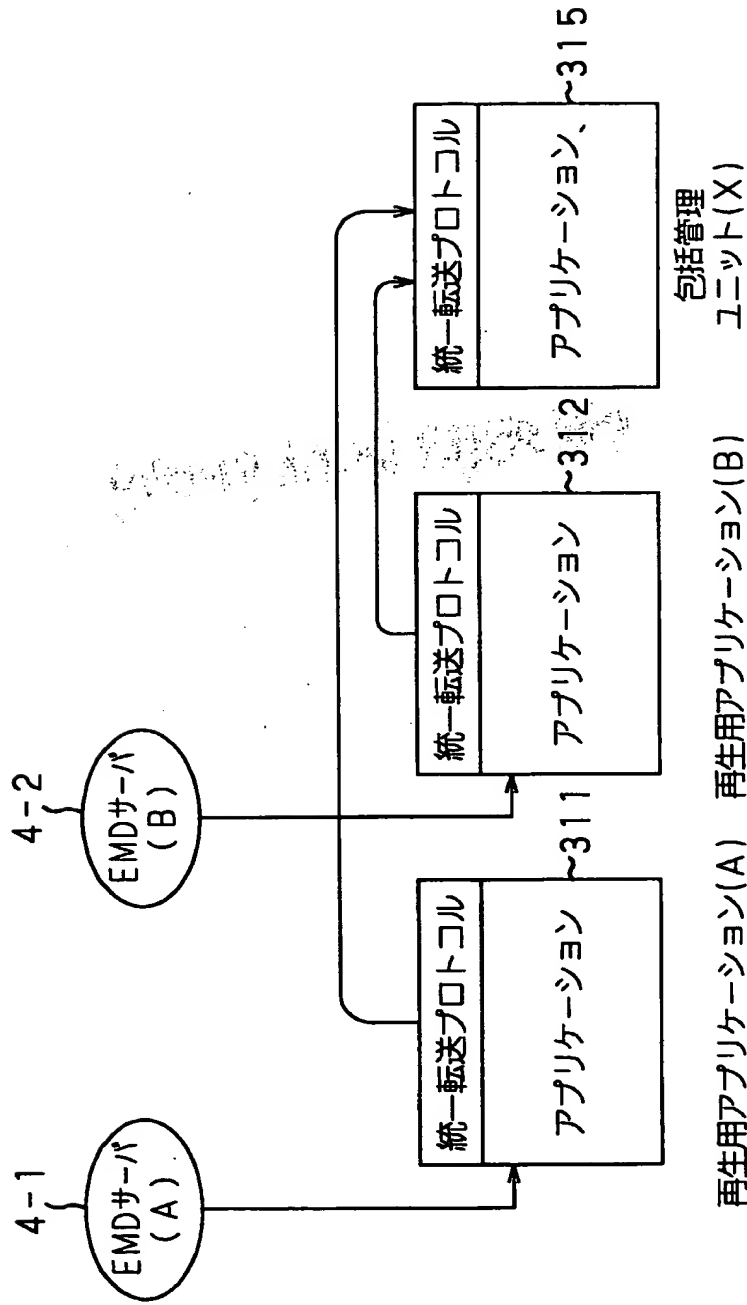


Fig. 8

This Page Blank (uspto)

9/26

Fig. 9A

ポリシー	値
from	99/10/25
to	99/11/24
pay/play	yes/10円

Fig. 9B

コンテンツ
利用条件情報

インデックスファイル	～331
オートマトンファイル	～332
パラメータファイル	～333
履歴ファイル	～334

Fig. 10

Automaton	～341
$MAC_{K_E}(\text{Automaton})$	～342
$Sig_{K_E}^{-1}(\text{Automaton})$	～343
$Cert(K_E^1)$	～344

Fig. 11

This Page Blank (uspto)

10/26

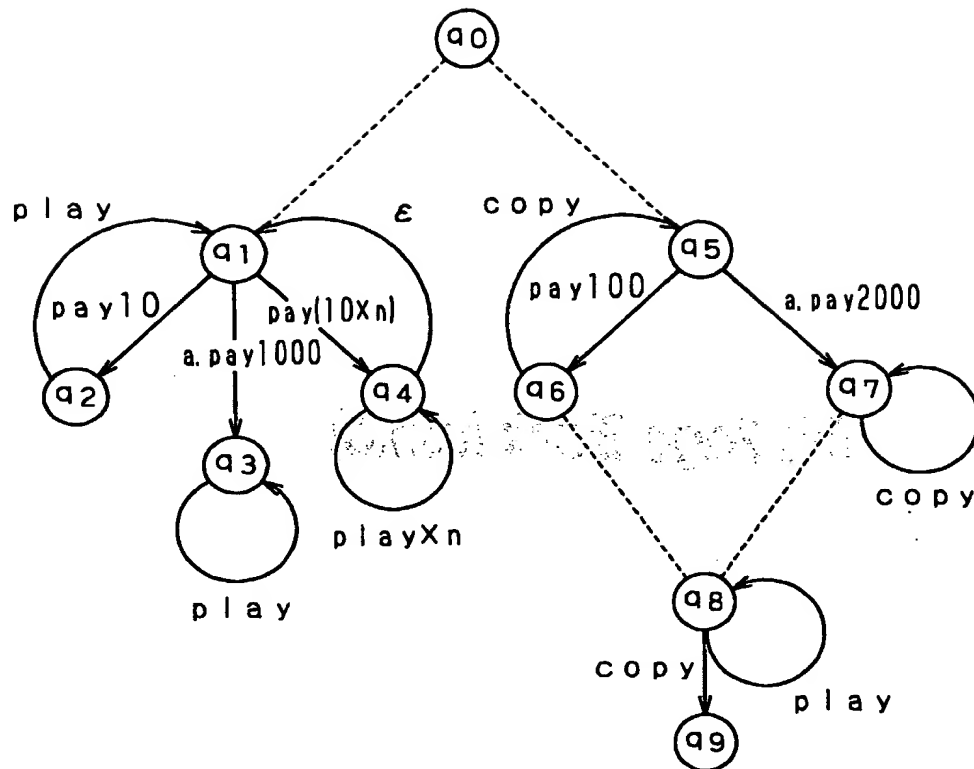


Fig. 12

This Page Blank (uspto)

11/26

$\langle q_1, \text{pay}10, q_2 \rangle$
 $\langle q_1, \text{a.pay}1000, q_3 \rangle$
 $\langle q_1, \text{pay}(10 \times n), q_4 \rangle$
 $\langle q_2, \text{play}, q_1 \rangle$
 $\langle q_3, \text{play}, q_3 \rangle$
 $\langle q_4, \text{play} \times n, q_4 \rangle$
 $\langle q_4, \epsilon, q_1 \rangle$
 $\langle q_5, \text{pay}100, q_6 \rangle$
 $\langle q_5, \text{a.pay}2000, q_7 \rangle$
 $\langle q_6, \text{copy}, q_5 \rangle$
 $\langle q_7, \text{copy}, q_7 \rangle$
 $\langle q_8, \text{play}, q_8 \rangle$
 $\langle q_8, \text{copy}, q_9 \rangle$

Fig.13

Entity ID	~ 345
Content ID	~ 346
Automaton Version	~ 347
Variables	~ 348
Tuples	~ 349
Automaton Version	~ 347
Variables	~ 348
Tuples	~ 349
⋮	

Fig.14

This Page Blank (uspto)

12/26

```
<!ENTITY % event" (  
    play  
    copy  
    pay-for-play  
    pay-for-copy  
    pay-for-album-play  
    pay-for-album-copy  
    from  
    to  
    null  
)" )
```

```
<!ENTITY % command" (  
    drop  
    dup  
    swap  
    add  
    subtract  
    multiply  
    divide  
    remainder  
    upper  
    lower  
    equal  
    less  
    greater  
    less-equal  
    greater-equal  
    and  
    or  
    not  
    bit-and  
    bit-or  
    bit-xor  
    bit-not  
)" )
```

Fi g.15

This Page Blank (uspto)

13/26

Content playable from 1999/9/1

```
<automaton>
  <!--This usage rule system has one Right Unit.
  Initial state is q1-->
  <initial-right-unit state="q1"/>
  <node state="q1">
    <!--If after 1999/9/1, transfer to q2-->
    <rule event="from" next-state="q2">
      <arguments>
        <integer value="time:19990901"/>
      </arguments>
    </rule>
  </node>
  <node state="q2">
    <!--Playable-->
    <rule event="play" next-state="q2"/>
  </node>
</automaton>
```

Fig. 16

This Page Blank (uspto)

14/26

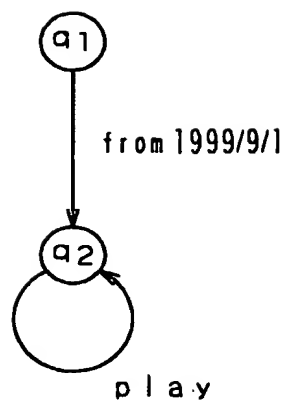


Fig. 17

This Page Blank (uspto)

15/26

Content playable until 1999/10/31

<automaton>

<!--This Usage Rule System has one Right Unit.

Initial state is q2-->

<initial-right-unit state="q2"/>

<node state="q2">

<!--If after 1999/10/31, transfer to end-->

<rule event="to" next-state="end">

<arguments>

<integer value="time:19991031"/>

</arguments>

</rule>

<!--Playable-->

<rule event="play" next-state="q2">

</rule>

</node>

<!--Unusable state-->

<node state="end"/>

</automaton>

Fi g.18

This Page Blank (uspto)

16/26

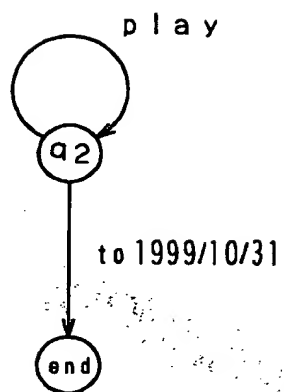


Fig. 19

This Page Blank (uspto)

17/26

Content playable 16 times 1999/9/1 to 1999/10/31

<automaton>

```
<!--Define counter variables for playable numbers. Initial value is 16-->
<define-variable name="count" initial-value="16"/>
```

```
<!--This Usage Rule System has one Right Unit. Initial state is q1-->
<initial-right-unit state="q1"/>
```

```
<node state="q1">
  <!--From 1999/9/1 transfer to q2-->
  <rule event="from" next-state="q2">
    <arguments>
      <integer value="time:19990901"/>
    </arguments>
  </rule>
</node>
```

```
<node state="q2">
  <!--From 1999/10/31 transfer to end-->
  <rule event="to" next-state="end">
    <arguments>
      <integer value="time:19991031"/>
    </arguments>
  </rule>
```

```
<rule event="play" next-state="q2">
  <!--playable only for "count" numbers-->
  <arguments>
    <variable name="count"/>
    <command name="load"/>
  </arguments>
  <!--If this rule is selected, the "count" number decrements by one-->
  <action>
    <variable name="count"/>
    <command name="load"/>
    <integer value="1"/>
    <command name="subtract"/>
    <variable name="count"/>
    <command name="store"/>
  </action>
</rule>
</node>
```

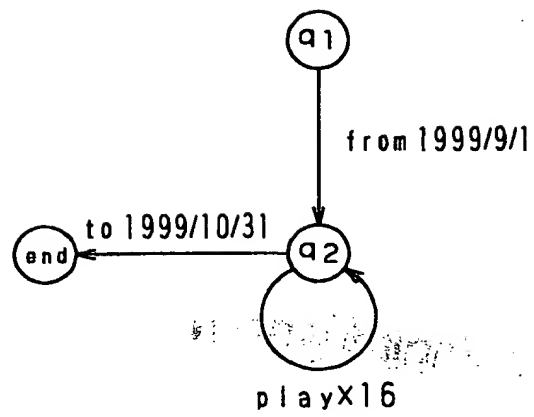
```
<!--Unusable state-->
<node state="end"/>
```

</automaton>

Fig. 20

This Page Blank (uspto)

18/26



Fi g.21

This Page Blank (uspto)

19/26

Content playable less than and/or equal to 16 times

<automaton>

```

<!--Define valuable counter for playable numbers.
Initial value is 16-->
<define-variable name="count" initial-value="16"/>

```

```

<!--Usage Rule System has one Right Unit.
Initial state is q2-->
<initial-right-unit state="q1"/>

```

```

<node state="q2">
  <rule event="play" next-state="q2">
    <!--"Count" number of times playable-->
    <arguments>
      <variable name="count"/>
      <command name="load"/>
    </arguments>
    <!--If this rule is selected, "count"
    number decrements by one-->
    <action>
      <variable name="count"/>
      <command name="load"/>
      <integer value "1"/>
      <command name="subtract"/>
      <variable name="count"/>
      <command name="store"/>
    </action>
  </rule>
</node>

```

</automaton>

Fig.22

This Page Blank (uspto)

20/26

Parameters	~ 351
$MAC_{K_c}(Parameters)$	~ 352
$Sig_{K_E^{-1}}(Parameters)$	~ 353
$Cert(K_E^1)$	~ 354

Fi g.23

Parameters	~ 351
Entity ID	~ 355
$MAC_{K_c}(Parameters)$	~ 352
$Sig_{K_E^{-1}}(Parameters)$	~ 353
$Cert(K_E^1)$	~ 354

Fi g.24

Entity ID	~ 356
Contents ID	~ 357
Contents	~ 358

Fi g.25

This Page Blank (uspto)

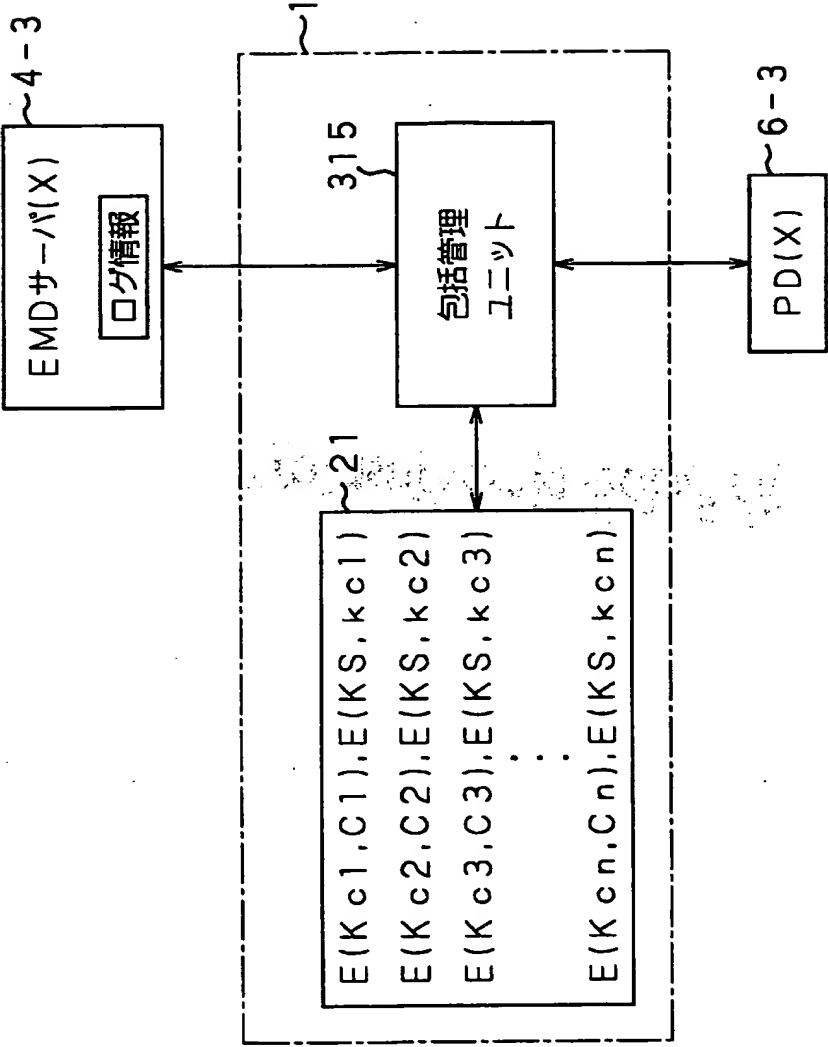


Fig. 26

This Page Blank (uspto)

22/26

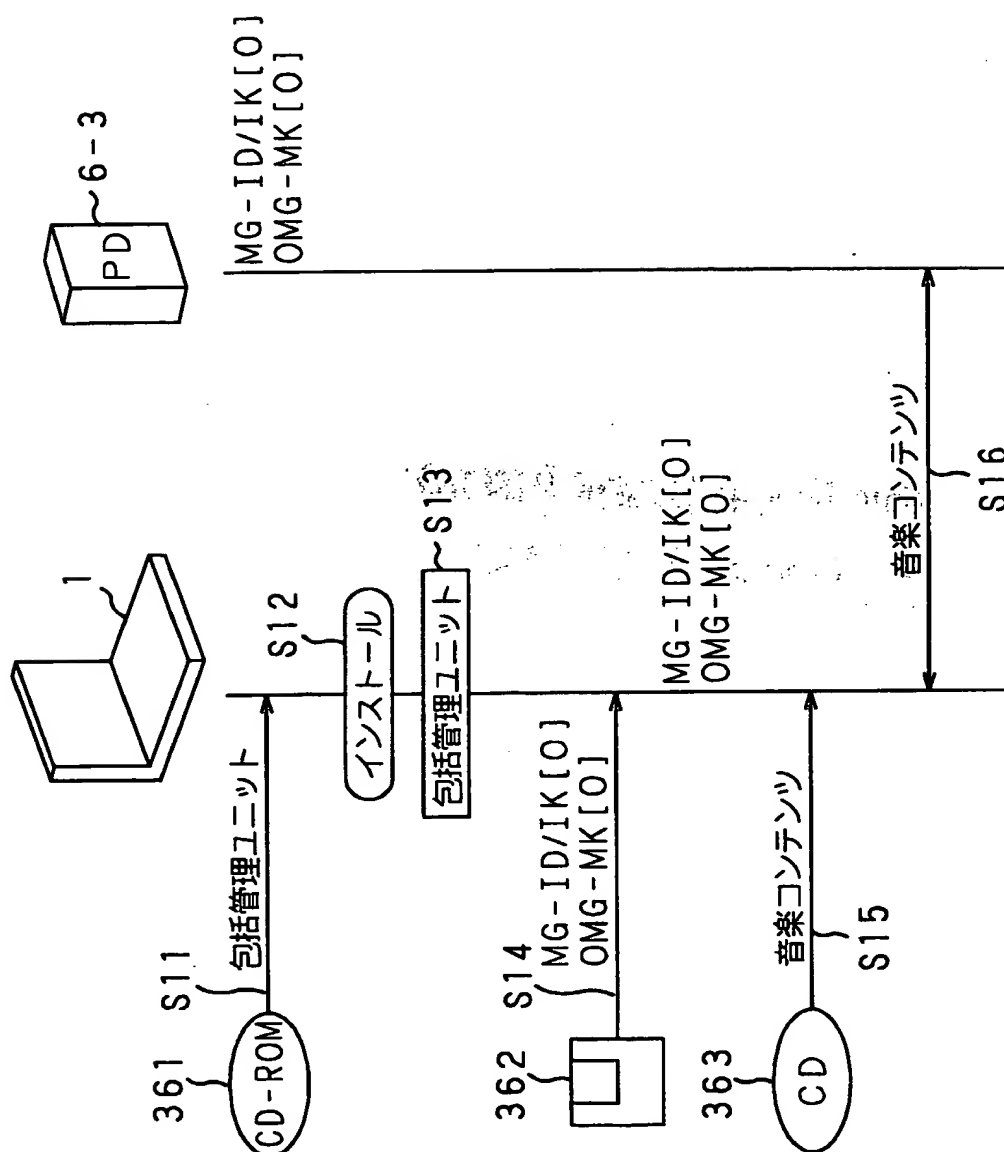


Fig. 27

This Page Blank (uspto)

23/26

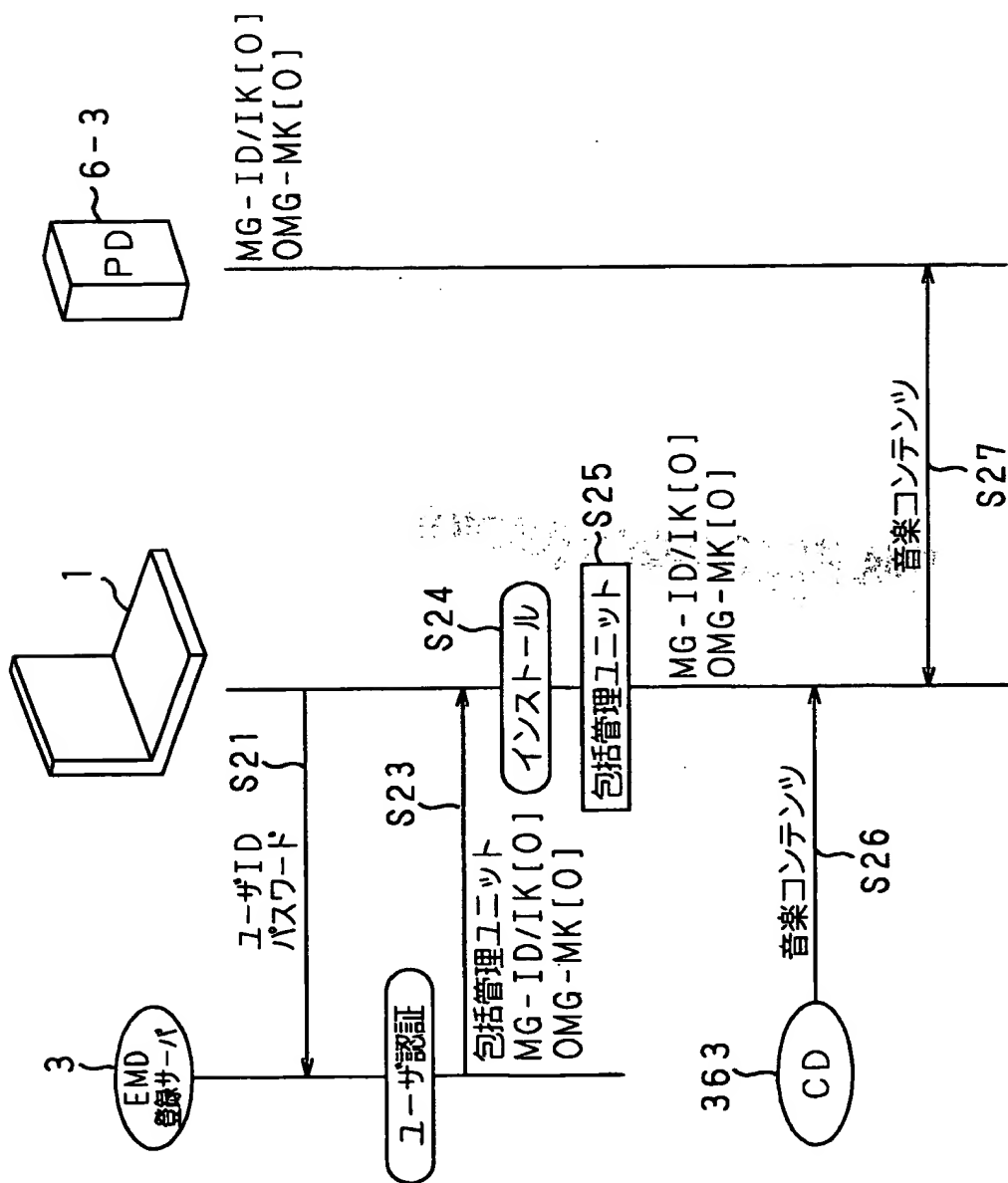


Fig. 28

This Page Blank (uspto)

24/26

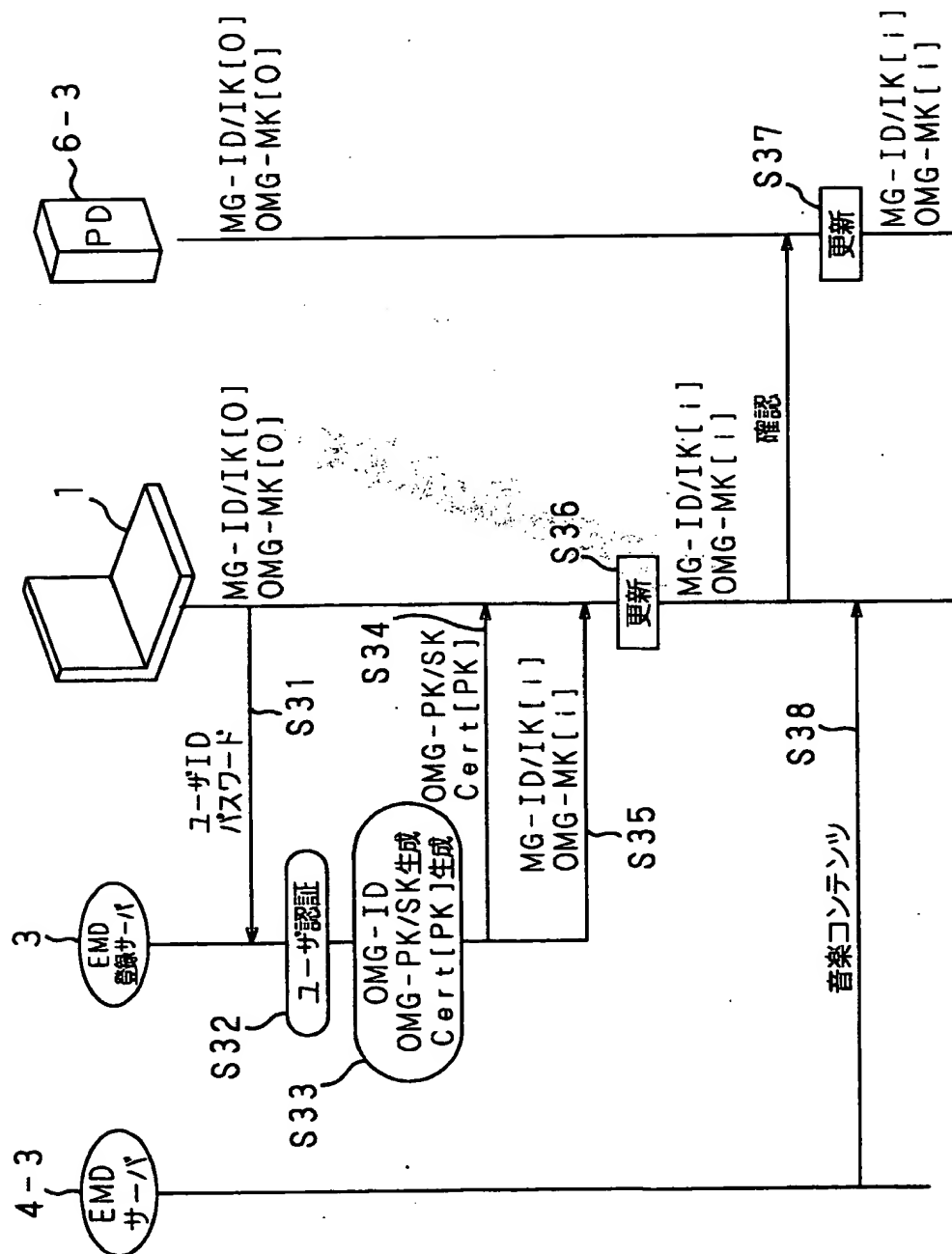


Fig. 29

This Page Blank (uspto)

25/26

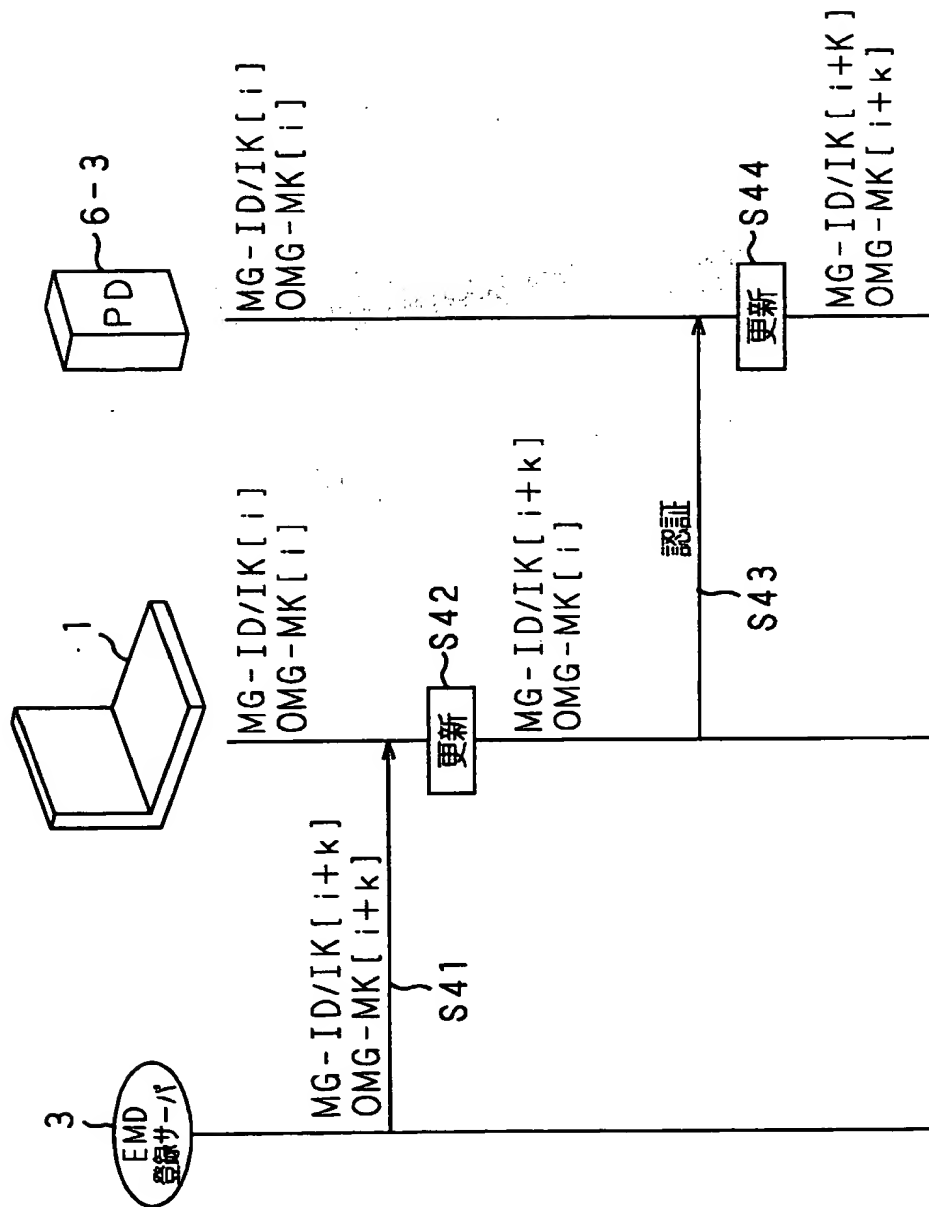


Fig.30

This Page Blank (uspto)

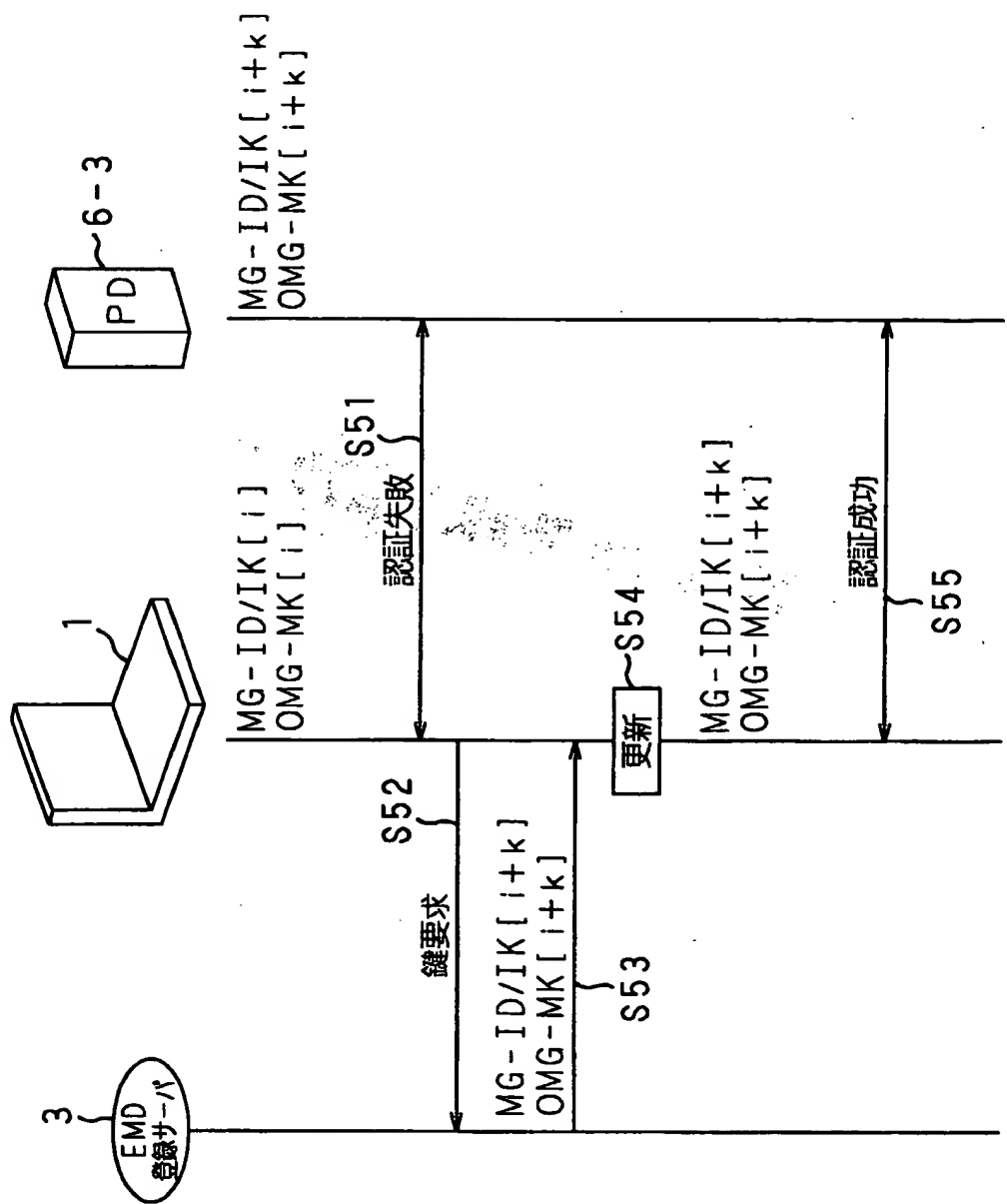


Fig.31

This Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/07473

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F15/00, H04L9/08, H04L9/32, G10K15/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F15/00, H04L9/08, H04L9/32, G10K15/02, G06F17/60, G11B 20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Toroku Jitsuyo Shinan Koho 1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, JICST Science Technology Document Database, INSPEC content, distribute, delivery, key, generation, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
EA	EP, 1001419, A1 (Matsushita Electric Ind. Co. Ltd.), 17 May, 2000 (17.05.00), Full text & WO, 2000/28539, A1 & JP, 2000-207835, A & BR, 9906815, A & NO, 200003492, A	1-10
EA	EP, 994404, A1 (Matsushita Electric Ind. Co. Ltd.), 19 April, 2000 (19.04.00), Full text & AU, 9952684, A & CN, 1263331, A & JP, 2000-348003, A	1-10
EA	JP, 2000-357201, A (Matsushita Electric Ind. Co., Ltd.), 26 December, 2000 (26.12.00), Full text (Family: none)	1-10
EA	JP, 2000-269950, A (Matsushita Electric Ind. Co., Ltd.), 29 September, 2000 (29.09.00), Full text (Family: none)	1-10

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
14 February, 2001 (14.02.01)

Date of mailing of the international search report
27 February, 2001 (27.02.01)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

This Page Blank (uspto)

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int. Cl ⁷ G06F15/00, H04L9/08, H04L9/32, G10K15/02		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int. Cl ⁷ G06F15/00, H04L9/08, H04L9/32, G10K15/02, G06F17/60, G11B 20/10		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1926-1996年		
日本国公開実用新案公報 1971-2001年		
日本国実用新案登録公報 1996-2001年		
日本国登録実用新案公報 1994-2001年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
WPI, JICST科学技術文献データベース, INSPEC content, distribute, delivery, key, generation, authentication		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
EA	EP, 1001419, A1 (Matsushita Electric Ind. Co. Ltd.) 17. 5月. 2000 (17. 05. 00), 全頁を参照 & WO, 2000/28539, A1 & JP, 2000-207835, A & BR, 9906815, A & NO, 200003492, A	1-10
EA	EP, 994404, A1 (Matsushita Electric Ind. Co. Ltd.) 19. 4月. 2000 (19. 04. 00), 全頁を参照 & AU, 9952684, A & CN, 1263331, A & JP, 2000-348003, A	1-10
EA	JP, 2000-357201, A (松下電器産業株式会社) 26. 12月. 2000 (26. 12. 00), 全頁を参照 (ファミリーなし)	1-10
<input checked="" type="checkbox"/> C欄の続きにも文献が列举されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日	14. 02. 01	国際調査報告の発送日
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 中里 裕正	5M 9364
		電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
E A	JP, 2000-269950, A (松下電器産業株式会社) 29. 09月. 2000 (29. 09. 00), 全頁を参照 (ファミリーなし)	1-10

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2001年5月3日 (03.05.2001)

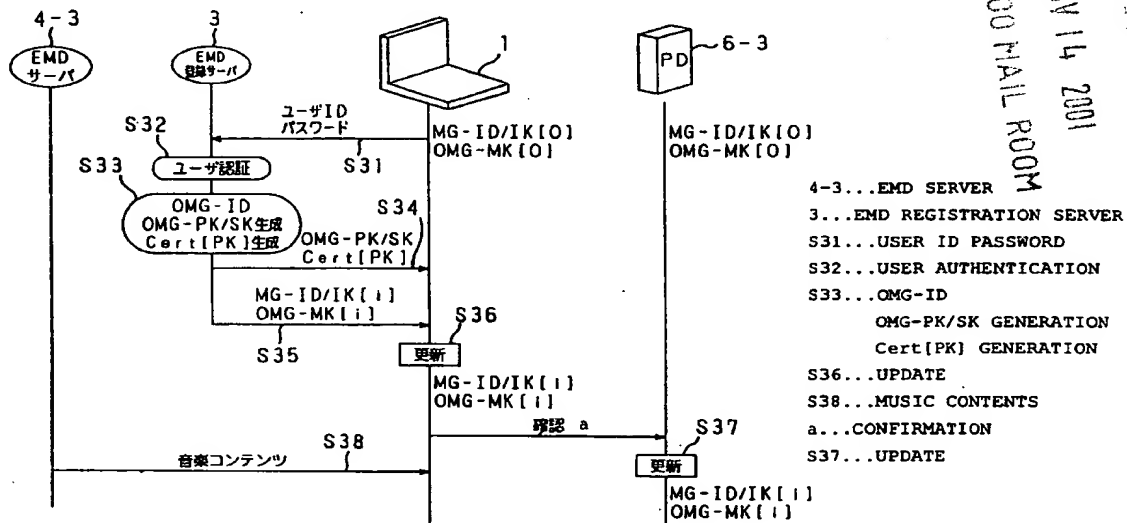
PCT

(10) 国際公開番号
WO 01/31461 A1

- (51) 国際特許分類: G06F 15/00, — (EZURA, Yuichi) [JP/JP]. 佐藤 一郎 (SATO, Ichiro) [JP/JP]. 海老原宗毅 (EBIHARA, Munetake) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (21) 国際出願番号: PCT/JP00/07473
- (22) 国際出願日: 2000年10月25日 (25.10.2000) (74) 代理人: 小池 晃, 外(KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語 (81) 指定国 (国内): CA, CN, KR, US.
- (30) 優先権データ: 特願平 11-303142 1999年10月25日 (25.10.1999) JP (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてののみ): 石黒隆二 (ISHIGURO, Ryuji) [JP/JP]. 河上 達 (KAWAKAMI, Itaru) [JP/JP]. 田辺 充 (TANABE, Mitsuru) [JP/JP]. 江面裕
- 添付公開書類:
— 国際調査報告書
— 補正書
- 補正されたクレームの公開日: 2001年10月18日
- 2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: CONTENTS PROVIDING SYSTEM

(54) 発明の名称: コンテンツ提供システム



(57) Abstract: A reproduction program is installed in a PC, and then a ripping key of a CD is provided from, e.g. an FD. By using the ripping key, the music contents in the CD can be copied to a PD, but music contents cannot be downloaded from an EMD server and copied to a PD. If the music contents distributed from an EMD server is stored in a PD, a key for EMD different from the ripping key is acquired through a network and the reproduction program is executed. Thus, the security of the contents data distributed through a network is enhanced.

[続葉有]

WO 01/31461 A1



(57) 要約:

再生プログラムは、P C上にインストールされた後に、C Dのリッピング用の鍵が例えばF Dから提供される。このC Dのリッピング用の鍵では、C D内の音楽コンテンツをP Dにコピーはできるが、E M Dサーバから音楽コンテンツをダウンロードしてP Dにコピーすることはできない。再生プログラムは、E M Dサーバから配信された音楽コンテンツをP Dに保存する場合には、リッピング用の鍵とは異なるE M D用の鍵をネットワークを介して取得したのちに行う。このようにすることにより、ネットワークを介して配信されたコンテンツデータの安全性を高められる。

補正書の請求の範囲

[2001年4月24日(24.04.01)国際事務局受理：新しい請求の範囲11-50が加えられた；他の請求の範囲は変更なし。(16頁)]

1. コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとからなるコンテンツ提供システムにおいて、

上記データ処理装置は、

上記再生プログラムがインストールされた後に、第1のマスター鍵及び第1の認証鍵が上記再生プログラムに提供され、上記第1のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第1の認証鍵及び第1のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、

上記再生プログラムが上記コンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第1のマスター鍵とは異なる第2のマスター鍵及び上記第1の認証鍵とは異なる第2の認証鍵がネットワークを介して提供され、この提供された第2のマスター鍵を用いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第2の認証鍵及び第2のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うこと

を特徴とするコンテンツ提供システム。

2. 上記可搬再生装置は、第1から第*i* (*i*は2以上の整数)世

代まで世代更新されていく第1から第 i の認証鍵、及び、第1から第 i (i は2以上の整数) 世代まで世代更新されていく第1から第 i のマスター鍵を保持しており、

上記再生プログラムは、第2から第 i (i は2以上の整数) まで世代更新されていく第2から第 i の認証鍵、及び、第2から第 i (i は2以上の整数) まで世代更新されていく第2から第 i のマスター鍵がネットワークを介して提供され、

上記可搬再生装置と上記再生プログラムとは、同一世代の認証鍵を用いて相互認証を行うこと

を特徴とする請求の範囲第1項記載のコンテンツ提供システム。

3. 上記可搬再生装置は、上記再生プログラムと認証を行った際に、この再生プログラムが用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記再生プログラムが用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求の範囲第2項記載のコンテンツ提供システム。

4. 上記再生プログラムは、上記可搬再生装置と認証を行った際に、上記可搬再生装置が用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記コンテンツサーバに鍵要求をして、上記可搬再生装置が用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求の範囲第2項記載のコンテンツ提供システム。

5. 上記コンテンツサーバは、上記再生プログラムからアクセスされた際に、上記再生プログラムが用いている認証鍵の世代よりも新しい世代の認証鍵及びマスター鍵を上記再生プログラムに提供して、上記再生プログラムが用いている認証鍵の世代更新をすること

を特徴とする請求の範囲第2項記載のコンテンツ提供システム。

6. コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置とによりユーザにコンテンツデータを提供するコンテンツサーバとからなるコンテンツ提供方法において、

上記再生プログラムをインストールした後に、第1のマスター鍵及び第1の認証鍵が上記再生プログラムに提供され、上記第1のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第1の認証鍵及び第1のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、

上記再生プログラムがコンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第1のマスター鍵とは異なる第2のマスター鍵及び上記第1の認証鍵とは異なる第2の認証鍵がネットワークを介して提供され、この提供された第2のマスター鍵を用いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第2の認証鍵及び第2のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うこと

を特徴とするコンテンツ提供方法。

7. 上記可搬再生装置が、第1から第 i (i は2以上の整数)世代まで世代更新されていく第1から第 i の認証鍵、及び、第1から第 i (i は2以上の整数)世代まで世代更新されていく第1から第 i のマスター鍵を保持しており、

上記再生プログラムは、第2から第 i （ i は2以上の整数）まで世代更新されていく第2から第 i の認証鍵、及び、第2から第 i （ i は2以上の整数）まで世代更新されていく第2から第 i のマスター鍵がネットワークを介して提供され、

上記可搬再生装置と上記再生プログラムとは、同一世代の認証鍵を用いて相互認証を行うこと

を特徴とする請求の範囲第6項記載のコンテンツ提供方法。

8. 上記可搬再生装置が、上記再生プログラムと認証を行った際に、この再生プログラムが用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記再生プログラムが用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求の範囲第7項記載のコンテンツ提供方法。

9. 上記再生プログラムが、上記可搬再生装置と認証を行った際に、上記可搬再生装置が用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記コンテンツサーバに鍵要求をして、上記可搬再生装置が用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求の範囲第7項記載のコンテンツ提供方法。

10. 上記コンテンツサーバが、上記再生プログラムからアクセスされた際に、上記再生プログラムが用いている認証鍵の世代よりも新しい世代の認証鍵及びマスター鍵を上記再生プログラムに提供して、上記再生プログラムが用いている認証鍵の世代更新をすること

を特徴とする請求の範囲第7項記載のコンテンツ提供方法。

11. （追加） 鍵データをデータ処理装置に提供する鍵データ提

供方法において、

コンテンツ再生プログラムがインストールされた上記データ処理装置に対して第1の鍵を提供し、

上記第1の鍵データは、外部記憶媒体に格納されたコンテンツデータを取得して上記データ処理装置に保存するのに用いられるとともに、上記データ処理装置に接続される可搬再生装置との上記コンテンツデータの送受信のための認証に用いられ、

上記可搬再生装置と、上記データ処理装置の上記コンテンツ再生プログラムが、コンテンツサーバから配信されるコンテンツデータの送受信を行う場合には、

上記第1の鍵データとは異なる第2の鍵データがネットワークを介して提供され、

上記第2の鍵データは、上記コンテンツサーバから提供されたコンテンツデータを取得して上記データ処理装置に保存するのに用いられるとともに、上記コンテンツサーバからのコンテンツデータの送受信を行うために、上記データ処理装置と上記可搬再生装置との認証に用いられてなること

を特徴とする鍵データ提供方法。

12. (追加) 上記可搬再生装置のID情報、第*i*世代の鍵データを上記データ処理装置に送信することにより、上記データ処理装置の鍵データを世代更新させるとともに、上記可搬再生装置のID情報に基づき当該可搬再生装置の鍵データも世代更新せしめることを特徴とする請求の範囲第11項記載の鍵データ提供方法。

13. (追加) 上記可搬再生装置は、第1から第*i* (*i*は2以上の整数) 世代まで世代更新されていく第1から第*i*の鍵データを

保持しており、

上記コンテンツ再生プログラムに、第2から第 i (i は2以上の整数)まで世代更新されていく第2から第 i の鍵データをネットワークを介して提供することにより、

上記可搬再生装置と上記コンテンツ再生プログラムとが、同一世代の認証鍵を用いて相互認証を行うようになすことを特徴とする請求の範囲第11項記載の鍵データ提供方法。

14. (追加) 上記コンテンツ再生プログラムからアクセスされた際に、上記コンテンツ再生プログラムが用いている鍵データの世代よりも新しい世代の鍵データを上記コンテンツ再生プログラムに提供して、上記コンテンツ再生プログラムが用いている認証鍵の世代更新を行わせることを特徴とする請求の範囲第11項記載の鍵データ提供方法。

15. (追加) 上記第1の鍵データは、コンパクトディスクからコンテンツをリッピングするためのリッピング鍵であることを特徴とする請求の範囲第11項記載の鍵データ提供方法。

16. (追加) 上記第2の鍵データは、コンテンツサーバからコンテンツをダウンロードするためのサーバ接続鍵であることを特徴とする請求の範囲第11項記載の鍵データ提供方法。

17. (追加) 上記第1の鍵データは、第1のマスター鍵及び第1の認証鍵を含み、

上記第2の鍵データは、第2のマスター鍵及び第2の認証鍵を含むようにしてなることを特徴とする請求の範囲第11項記載の鍵データ提供方法。

18. (追加) 上記第1の鍵データの供給は、外部記憶媒体に

より行われてなることを特徴とする請求の範囲第 1 1 項記載の鍵データ提供方法。

19. (追加) 上記第 1 の鍵データの供給は、サーバ装置により行われてなることを特徴とする請求の範囲第 1 1 項記載の鍵データ提供方法。

20. (追加) 上記第 2 の鍵データの供給は、サーバ装置により行われてなることを特徴とする請求の範囲第 1 1 項記載の鍵データ提供方法。

21. (追加) 鍵データをデータ処理装置に提供する鍵データ提供装置において、

コンテンツ再生プログラムがインストールされた上記データ処理装置に対して第 1 の鍵を送信する送信手段を有し、

上記第 1 の鍵データは、外部記憶媒体に格納されたコンテンツデータを取得して上記データ処理装置に保存するのに用いられるとともに、上記データ処理装置に接続される可搬再生装置との上記コンテンツデータの送受信のための認証に用いられ、

上記可搬再生装置と、上記データ処理装置の上記コンテンツ再生プログラムが、コンテンツサーバから配信されるコンテンツデータの送受信を行う場合には、

上記送信手段は、上記第 1 の鍵データとは異なる第 2 の鍵データがネットワークを介して提供するようになし、

上記第 2 の鍵データは、上記コンテンツサーバから提供されたコンテンツデータを取得して上記データ処理装置に保存するのに用いられるとともに、上記コンテンツサーバからのコンテンツデータの送受信を行うために、上記データ処理装置と上記可搬再生装置との

認証に用いられてなること

を特徴とする鍵データ提供装置。

22. (追加) コンテンツデータを再生するコンテンツ再生プログラムを有し、

外部記憶媒体及び可搬再生装置に接続され、

上記外部記憶媒体のコンテンツデータを取得するとともに、上記外部記憶媒体から提供されたコンテンツデータを上記可搬再生装置に提供するようになすデータ処理装置であって、

上記コンテンツ再生プログラムに提供され、上記外部記憶媒体から供給されるコンテンツデータを保存するのに用いられる第1の鍵データを用いて、上記外部記憶媒体に格納されたコンテンツデータを取得する際に認証を行って送受信を行い、

上記コンテンツ再生プログラムがコンテンツサーバから配信されたコンテンツデータの送受信を行う場合には、上記第1の鍵データとは異なる第2の鍵データがネットワークを介して提供され、この提供された第2の鍵データを用いて上記コンテンツサーバから提供されたコンテンツデータを取得する際に認証を行って送受信を行うこと

を特徴とするデータ処理装置。

23. (追加) 上記コンテンツ再生プログラムは、著作権管理を処理する包括管理ユニット内に含まれ、該包括管理ユニットは、外部記録媒体からインストールされることにより記憶されてなることを特徴とする請求の範囲第22項記載のデータ処理装置。

24. (追加) 上記包括管理ユニットのインストールとともに上記第1の鍵データであるところの0世代分の鍵データを入手する

ようになすことを特徴とする請求の範囲第23項記載のデータ処理装置。

25. (追加) 上記第1の鍵データの供給は、外部記憶媒体により行われてなることを特徴とする請求の範囲第22項記載のデータ処理装置。

26. (追加) 上記第1の鍵データの供給は、サーバ装置により行われてなることを特徴とする請求の範囲第22項記載のデータ処理装置。

27. (追加) 上記第2の鍵データの供給は、サーバ装置により行われてなることを特徴とする請求の範囲第22項記載のデータ処理装置。

28. (追加) 鍵データ提供サーバから入手された可搬再生装置のID情報、第*i*世代の鍵データを受信することにより鍵データを世代更新し、該可搬再生装置のID情報に基づき可搬再生装置に該鍵データを転送して、該可搬再生装置の鍵データも世代更新させるようになすことを特徴とする請求の範囲第22項記載のデータ処理装置。

29. (追加) 上記可搬再生装置の第(*i* + *k*)世代の鍵データの世代が、当該データ処理装置内に保存されている第*i*世代の鍵データの世代より大きい場合は、ネットワークを介して鍵データ提供サーバに新しい世代の鍵データを要求し、該鍵データ提供サーバから配信された第(*i* + *k*)世代の鍵データを受信することにより鍵データを世代更新させるようになすことを特徴とする請求の範囲第22項記載のデータ処理装置。

30. (追加) コンテンツデータを再生するコンテンツ再生ブ

プログラムを有し、

外部記憶媒体及び可搬再生装置に接続され、

上記外部記憶媒体のコンテンツデータを取得するとともに、上記外部記憶媒体から提供されたコンテンツデータを上記可搬再生装置に提供するようになすデータ処理装置に利用されるデータ処理方法であって、

上記コンテンツ再生プログラムに提供され、上記外部記憶媒体から供給されるコンテンツデータを保存するのに用いられる第1の鍵データを用いて、上記外部記憶媒体に格納されたコンテンツデータを取得する際に認証を行って送受信を行い、

上記コンテンツ再生プログラムがコンテンツサーバから配信されたコンテンツデータの送受信を行う場合には、上記第1の鍵データとは異なる第2の鍵データがネットワークを介して提供され、この提供された第2の鍵データを用いて上記コンテンツサーバから提供されたコンテンツデータを取得する際に認証を行って送受信を行うこと

を特徴とするデータ処理方法。

31. (追加) 上記コンテンツ再生プログラムは、著作権管理を処理する包括管理ユニット内に含まれ、該包括管理ユニットは、外部記録媒体からインストールされることにより記憶されてなることを特徴とする請求の範囲第30項記載のデータ処理方法。

32. (追加) 上記包括管理ユニットのインストールとともに上記第1の鍵データであるところの0世代分の鍵データを入手するようになすことを特徴とする請求の範囲第31項記載のデータ処理方法。

33. (追加) 上記第1の鍵データの供給は、外部記憶媒体により行われてなることを特徴とする請求の範囲第30項記載のデータ処理方法。

34. (追加) 上記第1の鍵データの供給は、サーバ装置により行われてなることを特徴とする請求の範囲第30項記載のデータ処理方法。

35. (追加) 上記第2の鍵データの供給は、サーバ装置により行われてなることを特徴とする請求の範囲第30項記載のデータ処理方法。

36. (追加) 鍵データ提供サーバから入手された可搬再生装置のID情報、第*i*世代の鍵データを受信することにより鍵データを世代更新し、該可搬再生装置のID情報に基づき可搬再生装置に該鍵データを転送して、該可搬再生装置の鍵データも世代更新させるようになることを特徴とする請求の範囲第30項記載のデータ処理方法。

37. (追加) 上記可搬再生装置の第(*i* + *k*)世代の鍵データの世代が、データ処理装置内に保存されている第*i*世代の鍵データの世代より大きい場合は、ネットワークを介して鍵データ提供サーバに新しい世代の鍵データを要求し、該鍵データ提供サーバから配信された第(*i* + *k*)世代の鍵データを受信することにより鍵データを世代更新させるようになることを特徴とする請求の範囲第30項記載のデータ処理方法。

38. (追加) コンテンツデータを再生するコンテンツ再生プログラムを有し、

外部記憶媒体及び可搬再生装置に接続され、

上記外部記憶媒体のコンテンツデータを取得するとともに、上記外部記憶媒体から提供されたコンテンツデータを上記可搬再生装置に提供するようになすデータ処理装置にて実行されるプログラムを格納した記憶媒体であって、

上記コンテンツ再生プログラムに提供され、上記外部記憶媒体から供給されるコンテンツデータを保存するのに用いられる第1の鍵データを用いて、上記外部記憶媒体に格納されたコンテンツデータを取得する際に認証を行って送受信を行い、

上記コンテンツ再生プログラムがコンテンツサーバから配信されたコンテンツデータの送受信を行う場合には、上記第1の鍵データとは異なる第2の鍵データがネットワークを介して提供され、この提供された第2の鍵データを用いて上記コンテンツサーバから提供されたコンテンツデータを取得する際に認証を行って送受信を行うように、上記データ処理装置に機能させるプログラムを格納してなること

を特徴とする記憶媒体。

39. (追加) コンテンツデータを再生するコンテンツ再生プログラムを有するデータ処理装置に接続され、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置であって、

予め固有のID情報及び複数世代分の上記鍵データが保存され、

上記データ処理装置内の上記コンテンツ再生プログラムに提供され、上記データ処理装置に接続された外部記憶媒体から供給されるコンテンツデータを保存するのに用いられる第1の鍵データと同世代の鍵データを用いて、該データ処理装置に接続された外部記憶媒

体に格納されたコンテンツデータを取得する際に上記データ処理装置と認証を行って送受信を行い、

上記コンテンツ再生プログラムがコンテンツサーバから配信されたコンテンツデータの送受信を行う場合に、上記データ処理装置は上記第1の鍵データとは異なる第2の鍵データがネットワークを介して提供され、この提供された第2の鍵データと同じ世代の鍵データを用いて、上記コンテンツサーバから提供された上記コンテンツデータを取得する際に認証を行い、該コンテンツデータを上記データ処理装置から受信すること

を特徴とする可搬再生装置。

40. (追加) 複数世代分の認証鍵及び複数世代分のマスター鍵が予め保存されてなることを特徴とする請求の範囲第39項記載の可搬再生装置。

41. (追加) 上記第1の鍵データは、コンパクトディスクからコンテンツデータをリッピングするためのリッピング鍵であり、該リッピング鍵により上記コンパクトディスクからコンテンツデータを取得可能となすことを特徴とする請求の範囲第39項記載の可搬再生装置。

42. (追加) 上記第2の鍵データは、サーバ装置からコンテンツデータをダウンロードするためのサーバ接続鍵であり、該サーバ接続鍵により上記サーバ装置からコンテンツデータを取得可能となすことを特徴とする請求の範囲第39項記載の可搬再生装置。

43. (追加) 上記コンテンツ再生プログラムと認証を行った際に、該コンテンツ再生プログラムが用いている世代よりも古い世代の鍵データを用いている場合には、上記コンテンツ再生プログラ

ムが用いている世代まで自己の鍵データの世代更新をすることを特徴とする請求の範囲第39項記載の可搬再生装置。

44. (追加) 第1から第 i (i は2以上の整数) 世代まで世代更新されていく第1から第 i の鍵データを保持しており、

上記コンテンツ再生プログラムにネットワークを介して提供された、第2から第 i (i は2以上の整数) 世代まで世代更新されていく第2から第 i の鍵データのうちの同一世代の鍵データを用いて、上記コンテンツ再生プログラムと相互認証を行うようになすことを特徴とする請求の範囲第39項記載の可搬再生装置。

45. (追加) コンテンツデータを再生するコンテンツ再生プログラムを有するデータ処理装置に接続され、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置に利用されるデータ処理方法であって、

予め上記可搬再生装置に保存された固有のID情報及び複数世代分の鍵データを利用してなり、

上記データ処理装置内の上記コンテンツ再生プログラムに提供され、上記データ処理装置に接続された外部記憶媒体から供給されるコンテンツデータを保存するのに用いられる第1の鍵データと同世代の鍵データを用いて、該データ処理装置に接続された外部記憶媒体に格納されたコンテンツデータを取得する際に上記データ処理装置と認証を行って上記外部記憶媒体に格納されたコンテンツデータの受信を行い、

上記コンテンツ再生プログラムがコンテンツサーバから配信されたコンテンツデータの送受信を行う場合に、上記データ処理装置は上記第1の鍵データとは異なる第2の鍵データがネットワークを介

して提供され、この提供された第2の鍵データと同じ世代の鍵データを用いて、上記コンテンツサーバから提供された上記コンテンツデータを取得する際に認証を行い、該コンテンツデータを上記データ処理装置から受信すること

を特徴とするデータ処理方法。

46. (追加) 上記第1の鍵データは、コンパクトディスクからコンテンツデータをリッピングするためのリッピング鍵であり、該リッピング鍵により上記コンパクトディスクからコンテンツデータを取得可能となすことを特徴とする請求の範囲第45項記載のデータ処理方法。

47. (追加) 上記第2の鍵データは、サーバ装置からコンテンツデータをダウンロードするためのサーバ接続鍵であり、該サーバ接続鍵により上記サーバ装置からコンテンツデータを取得可能となすことを特徴とする請求の範囲第45項記載のデータ処理方法。

48. (追加) 上記コンテンツ再生プログラムと認証を行った際に、該コンテンツ再生プログラムが用いている世代よりも古い世代の鍵データを用いている場合には、上記コンテンツ再生プログラムが用いている世代まで上記可搬再生装置の鍵データの世代更新をすることを特徴とする請求の範囲第45項記載のデータ処理方法。

49. (追加) 第1から第 i (i は2以上の整数) 世代まで世代更新されていく第1から第 i の鍵データを上記可搬再生装置が保持しており、

上記コンテンツ再生プログラムにネットワークを介して提供された、第2から第 i (i は2以上の整数) 世代まで世代更新されていく第2から第 i の鍵データのうちの同一世代の鍵データを用いて、

上記コンテンツ再生プログラムと相互認証を行うようになすことを特徴とする請求の範囲第45項記載のデータ処理方法。

50. (追加) コンテンツデータを再生するコンテンツ再生プログラムを有するデータ処理装置に接続され、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置にて実行されるプログラムを格納した記憶媒体であって、
予め上記可搬再生装置に保存された固有のID情報及び複数世代分の鍵データを利用してなり、

上記データ処理装置内の上記コンテンツ再生プログラムに提供され、上記データ処理装置に接続された外部記憶媒体から供給されるコンテンツデータを保存するのに用いられる第1の鍵データと同世代の鍵データを用いて、該データ処理装置に接続された外部記憶媒体に格納されたコンテンツデータを取得する際に上記データ処理装置と認証を行って上記外部記憶媒体に格納されたコンテンツデータの受信を行い、

上記コンテンツ再生プログラムがコンテンツサーバから配信されたコンテンツデータの送受信を行う場合に、上記データ処理装置は上記第1の鍵データとは異なる第2の鍵データがネットワークを介して提供され、この提供された第2の鍵データと同じ世代の鍵データを用いて、上記コンテンツサーバから提供された上記コンテンツデータを取得する際に認証を行い、該コンテンツデータを上記データ処理装置から受信するように、上記可搬再生装置に機能させるプログラムを格納したこと

を特徴とする記憶媒体。